

# Lattice Sparsification and the Approximate Closest Vector Problem

Daniel Dadush\*

Gábor Kun†

January 1, 2013

## Abstract

We give a deterministic algorithm for solving the  $(1 + \varepsilon)$  approximate Closest Vector Problem (CVP) on any  $n$  dimensional lattice and any norm in  $2^{O(n)}(1 + 1/\varepsilon)^n$  time and  $2^n \text{poly}(n)$  space. Our algorithm builds on the lattice point enumeration techniques of Micciancio and Voulgaris (STOC 2010) and Dadush, Peikert and Vempala (FOCS 2011), and gives an elegant, deterministic alternative to the “AKS Sieve” based algorithms for  $(1 + \varepsilon)$ -CVP (Ajtai, Kumar, and Sivakumar; STOC 2001 and CCC 2002). Furthermore, assuming the existence of a  $\text{poly}(n)$ -space and  $2^{O(n)}$  time algorithm for exact CVP in the  $l_2$  norm, the space complexity of our algorithm can be reduced to polynomial.

Our main technical contribution is a method for “sparsifying” any input lattice while approximately maintaining its metric structure. To this end, we employ the idea of random sublattice restrictions, which was first employed by Khot (FOCS 2003) for the purpose of proving hardness for Shortest Vector Problem (SVP) under  $l_p$  norms.

---

\*Georgia Tech. Atlanta, GA, USA. Email: dndadush@gatech.edu

†Courant Institute for Mathematical Sciences, NY, USA. Email: kungabor@cs.elte.hu

# 1 Introduction

An  $n$ -dimensional lattice  $\mathcal{L}$  is  $\{\sum_{i=1}^n z_i \mathbf{b}_i : z_i \in \mathbb{Z}, i \in [n]\}$  for some basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$  of  $\mathbb{R}^n$ . Given a lattice  $\mathcal{L}$  and norm  $\|\cdot\|$  in  $\mathbb{R}^n$ , the Shortest Vector Problem (SVP) is to find a shortest *nonzero*  $\mathbf{v} \in \mathcal{L}$  under  $\|\cdot\|$ . Given an additional target  $\mathbf{t} \in \mathbb{R}^n$ , the Closest Vector Problem (CVP) – the inhomogenous analog of SVP – is to find a closest  $\mathbf{v} \in \mathcal{L}$  to  $\mathbf{t}$ . Here, one often works with the  $\ell_2$  norm and other  $\ell_p$  norms, or most generally, with norms (possibly asymmetric) induced by a convex body  $K$  containing 0 in its interior, defined by  $\|\mathbf{x}\|_K = \inf\{s \geq 0 : \mathbf{x} \in sK\}$ .

The SVP and CVP on lattices are central algorithmic problems in the geometry of numbers, with applications to Integer Programming [Len83], factoring polynomials over the rationals [LLL82], cryptanalysis (e.g., [Odl90, JS98, NS01]), and much more. For different applications, one must often consider lattice problems expressed under a variety of norms. Decoding signals over a Gaussian channel is expressed as a CVP under  $\ell_2$  [VB99], computing simultaneous diophantine approximations is generally expressed as an SVP under  $\ell_\infty$  [FT87], Schnorr reduced factoring (under some unproven number theoretic assumptions) to an SVP under the  $\ell_1$  norm [Sch91], the Frobenius problem can be expressed as a lattice problem under an asymmetric simplicial norm [Kan92], the Integer Programming problem reduces to lattice problems under general norms [Kan87, DPV11], etc.

Much is known about the computational complexity of SVP and CVP, in both their exact and approximation versions. On the negative side, SVP is NP-hard (in  $\ell_2$ , under randomized reductions) to solve exactly, or even to approximate to within any constant factor [Ajt98, CN98, Mic98, Kho04]. Many more hardness results are known for other  $\ell_p$  norms and under stronger complexity assumptions than  $P \neq NP$  (see, e.g., [vEB81, Din00, RR06, HR07]). CVP is NP-hard to approximate to within  $n^{c/\log \log n}$  factors for some constant  $c > 0$  [ABSS93, DKRS98, Din00], where  $n$  is the dimension of the lattice. Therefore, we do not expect to solve (or even closely approximate) these problems efficiently in high dimensions. Still, algorithms providing weak approximations or having super-polynomial running times are the foundations for the many applications mentioned above.

Though the applications are often expressed using a variety of norms, the majority of the algorithmic work on SVP and CVP over the last quarter century has focused on the important case of the  $\ell_2$  norm. While there has been both tremendous practical and theoretical progress for  $\ell_2$  based solvers, progress on more general norms has been much slower (we overview this history below). Illustrative of this, for most of the problems mentioned above, the solution strategy has almost invariably been to approximate the problem via a reduction to  $\ell_2$ . In many cases, the desired computational problem requires only a “coarse” approximate solution to the underlying lattice problem (e.g. where a  $\text{poly}(n)$  or even  $2^{O(n)}$  factor approximation suffices), in which case approximation by  $\ell_2$  is often sufficient. In some cases however, the errors induced by the  $\ell_2$  approximation can result in a substantial increase in worst case running time or yield unusable results. As an example, with respect to the Integer Programming Problem (IP), in a sequence of works Dadush, Peikert and Vempala [DPV11, Dad12a] worked directly with norms induced by the continuous relaxation – avoiding direct ellipsoidal approximations – to reduce the complexity of solving an  $n$ -variable IP from  $2^{O(n)} n^{2n}$  (previous best using  $\ell_2$  techniques [HK10]) to  $2^{O(n)} n^n$ . From these considerations we see that the problem of developing effective algorithms for solving the SVP and CVP under general norms is motivated.

The algorithmic history of the SVP and CVP is long and rich. We relate the broad outlines here, highlighting the pertinent developments for general norms, and refer the reader to the following references [MG02, HPS11] for a more complete accounting. There are three main classes of methods for solving lattice problems: basis reduction, randomized sieving, and Voronoi cell based search.

**Basis reduction** combines both local search on lattice bases and lattice point enumeration. The cel-

celebrated LLL basis reduction algorithm [LLL82] and further extensions [Bab85, Sch87] give  $2^{n/\text{polylog}(n)}$  approximations to SVP and CVP under  $\ell_2$  in  $\text{poly}(n)$  time. General norm variants of basis reduction are explored in [LS92, KR95] and give similar approximation guarantees for SVP (though not CVP) as the  $\ell_2$  versions. However, bounds on the time complexity were only proved for fixed dimension (when the running time is polynomial). For exact SVP and CVP in the  $\ell_2$  norm, Kannan’s algorithm and its subsequent improvements [Kan87, Hel85, HS07] use basis reduction techniques to deterministically compute solutions in  $2^{O(n \log n)}$  time and  $\text{poly}(n)$  space.

This performance remained essentially unchallenged until the breakthrough **randomized “sieving”** algorithm of Ajtai, Kumar, and Sivakumar [AKS01], which gave a  $2^{O(n)}$ -time and -space randomized algorithm for exact SVP under  $\ell_2$ . The randomized sieving approach consists of sampling an exponential number of “perturbed” lattice points, and then iteratively clustering and combining them to give shorter and shorter lattice points. Subsequently, the randomized sieve was greatly extended to yield solutions for more general norms and for the more general problem of  $(1 + \varepsilon)$ -CVP. For exact SVP, the randomized sieve was extended (in the same time complexity) to  $\ell_p$  norms [BN07], arbitrary symmetric norms [AJ08], and to “near-symmetric”<sup>1</sup> norms [Dad12b]. For CVP, the randomized sieve was further used to give a  $(\frac{1}{\varepsilon})^n$ -time and -space algorithm for  $(1 + \varepsilon)$ -CVP under the  $\ell_2$  norm [AKS02, BN07],  $\ell_p$  norms [BN07], and near-symmetric norms [Dad12b]. We remark that near-symmetric norms appear naturally in the context of Integer Programming: the problem of finding a lattice point near the “center” of the continuous relaxation (which need not be symmetric) can be directly expressed as a CVP under a near-symmetric norm [Dad12b]. Lastly, for the specific case of  $\ell_\infty$ , Eisenbrand, Hähnle and Niemeier [EHN11] show that  $(1 + \varepsilon)$ -CVP under  $\ell_\infty$  can be solved using  $O(\ln \frac{1}{\varepsilon})^n$  calls to any 2-approximate solver via an elegant cube covering technique. It is worth noting that AKS sieve based algorithms are *Monte Carlo*: while they output correct solutions (i.e. a shortest or closest vectors) with high probability, the correctness is not guaranteed.

In a major breakthrough, Micciancio and Voulgaris [MV10] gave a *deterministic*  $2^{O(n)}$ -time and -space algorithm for exact SVP and CVP under the  $\ell_2$  norm using the **Voronoi cell** of a lattice. The Voronoi cell, the symmetric polytope consisting of all points in space closer to the origin (under  $\ell_2$ ) than any other lattice point, is represented algorithmically here by  $O(2^n)$  lattice points corresponding to the facets of the Voronoi cell (known as Voronoi relevant vectors). The relevant vectors form an “extended basis” for the lattice which Micciancio and Voulgaris (MV) use to efficiently guide closest lattice point search. Though it is tempting to try and directly extend the MV techniques to other norms this appears to be quite challenging. A major difficulty is that for general norms the Voronoi cell need not be convex, and furthermore no good bounds are known for the number of relevant vectors. In a subsequent work however, Dadush, Peikert and Vempala [DPV11] showed that MV lattice point search techniques can, in a qualified sense, be extended to general norms (in fact, to general convex bodies) via a direct reduction to  $\ell_2$ . Combining a technique for constructing “efficient” ellipsoid coverings – using the M-Ellipsoid concept from convex geometry – together with Voronoi cell based search, they showed that the lattice points inside a convex body can be computed in time proportional to the maximum number of lattice points the body can contain in any translation. With some further improvements [DV12, Dad12a], the DPV lattice point enumeration technique was used to give the first deterministic  $2^{O(n)}$ -time and -space algorithms for SVP and Bounded Distance Decoding (BDD)<sup>2</sup> under near-symmetric norms.

Despite all the recent progress, the only algorithms currently available for solving  $(1 + \varepsilon)$ -CVP under non-euclidean norms remain the AKS sieve based approaches. In this light, a main open problem from [DPV11] was to understand whether the DPV lattice point enumeration approach could be extended to work for

<sup>1</sup>An asymmetric norm with unit ball  $K \subseteq \mathbb{R}^n$  is near-symmetric if  $\text{vol}_n(K) \leq 2^{O(n)} \text{vol}_n(K \cap -K)$ .

<sup>2</sup>BDD is CVP when the distance to the target is guaranteed to be at most some factor times the minimum distance of the lattice.

$(1 + \varepsilon)$ -CVP under general norms.

## 1.1 Results and Techniques

Our main result is as follows:

**Theorem 1.1** (Approximate CVP in any norm, informal). *There is a deterministic algorithm that, given any near-symmetric norm  $\|\cdot\|_K$ ,  $n$  dimensional lattice  $\mathcal{L}$ , target  $\mathbf{x} \in \mathbb{R}^n$ , and  $0 < \varepsilon \leq 1$ , computes  $\mathbf{y} \in \mathcal{L}$ , a  $(1 + \varepsilon)$ -approximate minimizer to  $\|\mathbf{y} - \mathbf{x}\|_K$ , in  $(1 + \frac{1}{\varepsilon})^n \cdot 2^{O(n)}$  time and  $\tilde{O}(2^n)$  space.*

In the above theorem we extend the DPV lattice point enumeration techniques and give the first deterministic alternative to the AKS randomized sieving approach. Compared to AKS, our approach also achieves a better dependence on  $\varepsilon$ ,  $2^{O(n)}(1 + \frac{1}{\varepsilon})^n$  instead of  $2^{O(n)}(1 + \frac{1}{\varepsilon})^{2n}$ , and utilizes significantly less space,  $\tilde{O}(2^n)$  compared to  $2^{O(n)}(1 + \frac{1}{\varepsilon})^n$ . Additionally, as we will discuss below, continued progress on exact CVP under  $\ell_2$  could further reduce the space usage of the algorithm. We note however that the  $2^{O(n)}$  factors in the running time are currently much larger than in AKS, though little effort has been spent in trying to compute or optimize them. To explain our approach, we first present the main DPV enumeration algorithm in its most recent formulation [Dad12a].

**Theorem 1.2** (Enumeration in Convex Bodies, informal). *There is a deterministic algorithm that, given an  $n$ -dimensional convex body  $K$  and lattice  $\mathcal{L}$ , enumerates the elements of  $K \cap \mathcal{L}$  in time  $2^{O(n)}G(K, \mathcal{L})$  using  $\tilde{O}(2^n)$  space, where  $G(K, \mathcal{L}) = \max_{\mathbf{x} \in \mathbb{R}^n} |(K + \mathbf{x}) \cap \mathcal{L}|$ . Furthermore, given an algorithm that solves exact CVP under  $\ell_2$  in  $T(n)$  time and  $S(n)$  space,  $K \cap \mathcal{L}$  can be enumerated in  $2^{O(n)}T(n)G(K, \mathcal{L})$  time using  $S(n) + \text{poly}(n)$  space.*

The main idea for the above algorithm is to first compute a covering of  $K$  by  $2^{O(n)}$  translates of an  $M$ -ellipsoid  $E$  of  $K$ <sup>3</sup>, and to use the MV enumeration techniques to compute the lattice points inside each translate of  $E$ . In its first incarnation [DPV11], the above algorithm was randomized – here randomization was needed to construct the  $M$ -Ellipsoid – and had space complexity dependent on  $G(K, \mathcal{L})$ . In [DV12], a deterministic  $M$ -Ellipsoid construction was presented yielding a completely deterministic enumerator. Lastly in [Dad12a], the space usage was decoupled from  $G(K, \mathcal{L})$  and a direct reduction from lattice point enumeration to exact CVP under  $\ell_2$  was presented.

The above lattice point enumerator will form the core of our  $(1 + \varepsilon)$ -CVP algorithm. As we will see from the algorithm’s analysis, its space usage will only be an additive polynomial factor larger than the space required for the enumeration. Therefore, if one could develop an exact CVP solver under  $\ell_2$  which runs in  $2^{O(n)}$  time and  $\text{poly}(n)$  space, then the space usage of our  $(1 + \varepsilon)$ -CVP can be reduced to  $\text{poly}(n)$  in the same time complexity. The possibility of such a solver is discussed in [MV10] and developing it remains an important open problem. We remark that by plugging in Kannan’s algorithm for CVP under  $\ell_2$ , we do indeed get a  $\text{poly}(n)$  space  $(1 + \varepsilon)$ -CVP solver, though at the cost of an  $n^{n/2}$  factor increase in running time.

Using the above enumerator as a blackbox, we now present the approach taken in [DPV11] to solve CVP and explain the main problem that arises. Given the target  $\mathbf{t} \in \mathbb{R}^n$ , their algorithm first computes an initial coarse underestimate  $d_0$  of the distance of  $\mathbf{t}$  to  $\mathcal{L}$  under  $\|\cdot\|_K$  (using LLL for example). For the next step, they use the lattice point enumerator to successively compute the sets  $(\mathbf{t} + 2^i d_0 K) \cap \mathcal{L}$  (i.e. all lattice points at distance at most  $2^i d_0$  from  $\mathbf{t}$ ),  $i \geq 0$ , until a lattice point is found. Finally, the closest vector to  $\mathbf{t}$  in the final enumerated set is returned.

---

<sup>3</sup>An  $M$ -Ellipsoid  $E$  of  $K$  satisfies that  $2^{O(n)}$  translates of  $E$  suffice to cover  $K$  and vice versa.

From the description, it is relatively straightforward to show that the complexity of the algorithm is essentially  $G(dK, \mathcal{L})$ , where  $d$  is the distance of  $\mathbf{t}$  to  $\mathcal{L}$ . The main problem with this approach is that, in general, one cannot apriori bound  $G(dK, \mathcal{L})$ ; even in 2 dimension this quantity can be made arbitrarily large. The only generic setting where such a bound is indeed available is when the distance  $d$  of the target is bounded by  $\alpha\lambda$ , where  $\lambda$  is the length of the shortest non-zero vector under  $\|\cdot\|_K$ . In this situation, we can bound  $G(dK, \mathcal{L})$  by  $2^{O(n)}(1+\alpha)^n$ . We remark that solving CVP with this type of guarantee corresponds to the Bounded Distance Problem problem in the literature, and by a standard reduction can be used to solve SVP in general norms as well [GMSS99].

To circumvent the above problem, we propose the following simple solution. Instead of solving the CVP on the original lattice  $\mathcal{L}$ , we attempt to solve it on a sparser sublattice  $\mathcal{L}' \subseteq \mathcal{L}$ , where the distance of  $\mathbf{t}$  to  $\mathcal{L}'$  is not much larger than its distance to  $\mathcal{L}$  (we settle for an approximate solution here) and where the maximum number of lattice points at the new target distance is appropriately bounded. Our main technical contribution is to show the existence of such “lattice sparsifiers” and give a deterministic algorithm to compute them:

**Theorem 1.3** (Lattice Sparsifier, informal). *There is a deterministic algorithm that, given any near-symmetric norm  $\|\cdot\|_K$ ,  $n$  dimensional lattice  $\mathcal{L}$ , and distance  $t \geq 0$ , computes a sublattice  $\mathcal{L}' \subseteq \mathcal{L}$  in deterministic  $2^{O(n)}$  time and  $\tilde{O}(2^n)$  space satisfying: (1) the distance from  $\mathcal{L}'$  to any point in  $\mathbb{R}^n$  is at most its distance to  $\mathcal{L}$  plus an additive  $t$ , (2) the number of points in  $\mathcal{L}'$  at distance  $t$  is at most  $2^{O(n)}$ .*

To solve  $(1+\varepsilon)$ -CVP using the above lattice sparsifier is straightforward. We simply compute a sparsifier  $\mathcal{L}'$  for  $\mathcal{L}$  under  $\|\cdot\|_K$  with  $t = \varepsilon d_K(t, \mathcal{L})$  (the distance from  $\mathbf{t}$  to  $\mathcal{L}$ ), and then solve the exact CVP on  $\mathcal{L}'$  using the DPV algorithm. By the guarantees on the sparsifier,  $\mathcal{L}'$  contains a point at distance at most  $d + \varepsilon d = (1 + \varepsilon)d$ , and using a simple packing argument (see Lemma 2.1) we can show that

$$G((1 + \varepsilon)d, \mathcal{L}') = 2^{O(n)}(1 + \frac{1}{\varepsilon})^n G(\varepsilon d, \mathcal{L}') = 2^{O(n)}(1 + \frac{1}{\varepsilon})^n.$$

Here we note that the correctness of the output follows from the distance preserving properties of  $\mathcal{L}'$ , and the desired runtime follows from the above bound on  $G((1 + \varepsilon)d, \mathcal{L}')$ .

To prove the existence of lattice sparsifier’s we make use of random sublattice restrictions, a tool first employed by Khot [Kho03, Kho04] for the purpose of proving hardness of SVP. More precisely, we show that with constant probability the restriction of  $\mathcal{L}$  by a random modular form (for an appropriately chosen modulus) yields the desired sparsifier. We remark that our use of sublattice restrictions is somewhat more refined than in [Kho03, Kho04]. In Khot’s setting, the random sublattice is calibrated to remove all short vectors on a NO instance, and to keep at least one short vector for a YES instance. In our setting, we somehow need both properties simultaneously for the *same* lattice, i.e. we want to remove many short vectors to guarantee reasonable enumeration complexity, while at the same time keeping enough vectors so that the original lattice lies “close” to the sublattice. As a final difference, we show that our construction can be derandomized in  $2^{O(n)}$  time, yielding a completely deterministic algorithm.

**Organization.** In section 3, we provide the exact reduction from  $(1 + \varepsilon)$ -CVP to lattice sparsification, formalizing Theorem 1.1. In section 4, we prove the existence of lattice sparsifiers using the probabilistic method. In section 5, we give the derandomized lattice sparsifier construction, formalizing Theorem 1.3. Lastly, in section 6, we discuss further applications and future directions.

## 2 Preliminaries

**Convexity and Norms.** For sets  $A, B \subseteq \mathbb{R}^n$ , let  $A+B = \{a+b : a \in A, b \in B\}$  denote their Minkowski sum.  $B_2^n$  denotes the  $n$ -dimensional euclidean unit ball in  $\mathbb{R}^n$ . A convex body  $K \subseteq \mathbb{R}^n$  is a full dimensional compact, convex set. A convex body  $K$  is  $(\mathbf{a}_0, r, R)$ -centered if  $\mathbf{a}_0 + rB_2^n \subseteq K \subseteq \mathbf{a}_0 + RB_2^n$ . For a convex body  $K \subseteq \mathbb{R}^n$  containing  $\mathbf{0}$  in its interior, we define the (possibly asymmetric) norm  $\|\cdot\|_K$  induced by  $K$  as  $\|\mathbf{x}\|_K = \inf\{s \geq 0 : \mathbf{x} \in sK\}$ . For a  $(\mathbf{0}, r, R)$ -centered convex body  $K$ , we note that  $\frac{1}{R}\|\mathbf{x}\|_2 \leq \|\mathbf{x}\|_K \leq \frac{1}{r}\|\mathbf{x}\|_2$ .

If  $K$  is symmetric ( $K = -K$ ), then  $\|\cdot\|_K$  is also symmetric ( $\|\mathbf{x}\|_K = \|\mathbf{x}\|_{-K}$ ), and hence defines a regular norm on  $\mathbb{R}^n$ . The convex body  $K$  ( $\|\cdot\|_K$ ) is  $\gamma$ -symmetric for  $\gamma \in (0, 1]$ , if  $\text{vol}_n(K \cap -K) \geq \gamma^n \text{vol}_n(K)$ .  $K$  is near-symmetric if it is  $\Omega(1)$ -symmetric.

**Computational Model.** The convex bodies and norms will be presented to our algorithms via weak membership and distance oracles. For  $\varepsilon \geq 0$  and  $K \subseteq \mathbb{R}^n$  a convex body, we define  $K^\varepsilon = K + \varepsilon B_2^n$  and  $K^{-\varepsilon} = \{\mathbf{x} \in K : \mathbf{x} + \varepsilon B_2^n \subseteq K\}$ . A *weak membership oracle*  $O_K$  for  $K$  is a function which takes as input a point  $\mathbf{x} \in \mathbb{Q}^n$  and real  $\varepsilon > 0$ , and returns  $O_K(\mathbf{x}, \varepsilon) = 1$  if  $\mathbf{x} \in K^{-\varepsilon}$ , 0 if  $\mathbf{x} \notin K^\varepsilon$ , and either 0 or 1 if  $\mathbf{x} \in K^\varepsilon \setminus K^{-\varepsilon}$ . A *weak distance oracle*  $D_K$ , for  $K$  is a function that takes as input a point  $\mathbf{x} \in \mathbb{Q}^n$  and  $\varepsilon > 0$ , and returns a rational number satisfying  $|D_{K,\varepsilon}(\mathbf{x}) - \|\mathbf{x}\|_K| \leq \varepsilon \min\{1, \|\mathbf{x}\|_K\}$ . The runtimes of our algorithms will be measured by the number of oracle calls and arithmetic operations. For simplicity, we use the notation  $\text{poly}(\cdot)$  to denote a polynomial factor in all the relevant input parameters (dimension, encoding length of basis, etc.).

**Lattices.** An  $n$ -dimensional lattice  $\mathcal{L} \subset \mathbb{R}^n$  is a discrete subgroup of  $\mathbb{R}^n$ ;  $\mathcal{L}$  can be expressed as  $B\mathbb{Z}^n$ , where  $B \in \mathbb{R}^{n \times n}$  is a non-singular matrix, which we refer to as a basis for  $\mathcal{L}$ . The dual lattice of  $\mathcal{L}$  is  $\mathcal{L}^* = \{\mathbf{y} \in \mathbb{R}^n : \forall \mathbf{x} \in \mathcal{L} \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}\}$ , which can be generated by the basis  $B^{-T}$  (inverse transpose).

We define the length of the shortest non-zero vector of  $\mathcal{L}$  under  $\|\cdot\|_K$  by  $\lambda_1(K, \mathcal{L}) = \min_{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{y}\|_K$ . We let  $\text{SVP}(K, \mathcal{L}) = \arg \min_{\mathbf{z} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{z}\|_K$  denote the set of shortest non-zero vectors of  $\mathcal{L}$  under  $\|\cdot\|_K$ . For  $\mathbf{x} \in \mathbb{R}^n$ , define the distance of  $\mathbf{x}$  to  $\mathcal{L}$  under  $\|\cdot\|_K$  by  $d_K(\mathcal{L}, \mathbf{x}) = \min_{\mathbf{y} \in \mathcal{L}} \|\mathbf{y} - \mathbf{x}\|_K$ . We let  $\text{CVP}(K, \mathcal{L}, \mathbf{x}) = \arg \min_{\mathbf{y} \in \mathcal{L}} \|\mathbf{y} - \mathbf{x}\|_K$  denote the set of closest vectors to  $\mathbf{x}$  in  $\mathcal{L}$  under  $\|\cdot\|_K$ .

For a lattice  $\mathcal{L}$  and convex body  $K$  in  $\mathbb{R}^n$ , let  $G(K, \mathcal{L})$  be the largest number of lattice points contained in any translate of  $K$ , that is  $G(K, \mathcal{L}) = \max_{\mathbf{x} \in \mathbb{R}^n} |(K + \mathbf{x}) \cap \mathcal{L}|$ . We will need the following bounds on  $G(K, \mathcal{L})$  from [Dad12a] (we include a proof in the appendix for completeness).

**Lemma 2.1.** *Let  $K \subseteq \mathbb{R}^n$  denote a  $\gamma$ -symmetric convex body and let  $\mathcal{L}$  denote an  $n$ -dimensional lattice. Then for  $d > 0$  we have that*

$$G(dK, \mathcal{L}) \leq \gamma^{-n} \left(1 + \frac{2d}{\lambda_1(K \cap -K, \mathcal{L})}\right)^n \quad \text{and} \quad G(dK, \mathcal{L}) \leq \gamma^{-n} (2d+1)^n \cdot |(K \cap -K) \cap \mathcal{L}|.$$

**Algorithms.** We will need the following lattice point enumeration algorithm from [DPV11, Dad12a].

**Theorem 2.2** (Algorithm Lattice-Enum( $K, \mathcal{L}, \varepsilon$ )). *Let  $K \subseteq \mathbb{R}^n$  be a  $(\mathbf{a}_0, r, R)$ -centered convex body given by weak membership oracle  $O_K$ , let  $\mathcal{L} \subseteq \mathbb{R}^n$  be an  $n$ -dimensional lattice with basis  $B \in \mathbb{Q}^{n \times n}$  and let  $\varepsilon > 0$ . Then there is a deterministic algorithm that on inputs  $K, \mathcal{L}, \varepsilon$  outputs a set  $S$  (one element at a time) satisfying*

$$K \cap \mathcal{L} \subseteq S \subseteq (K + \varepsilon B_2^n) \cap \mathcal{L}$$

*in  $G(K, \mathcal{L}) \cdot 2^{O(n)} \cdot \text{poly}(\cdot)$  time using  $2^n \text{poly}(\cdot)$  space.*

We will require the following SVP solver from [DPV11, Dad12a].

**Theorem 2.3** (Algorithm Shortest-Vectors( $K, \mathcal{L}, \varepsilon$ )). *Let  $K \subseteq \mathbb{R}^n$  be a  $(\mathbf{a}_0, r, R)$ -centered symmetric convex body given by weak membership oracle  $O_K$ , and let  $\mathcal{L} \subseteq \mathbb{R}^n$  be an  $n$ -dimensional lattice with basis  $B \in \mathbb{Q}^{n \times n}$ , and let  $\varepsilon > 0$ . Let  $\lambda_1 = \lambda_1(K, \mathcal{L})$ . Then there is an algorithm that on inputs  $K, \mathcal{L}, \varepsilon$  outputs a set  $S \subseteq \mathcal{L}$  satisfying*

$$\text{SVP}(K, \mathcal{L}) \subseteq S \subseteq \{\mathbf{y} \in \mathcal{L} \setminus \{\mathbf{0}\} : \|\mathbf{y}\|_K \leq \lambda_1 + \varepsilon \min\{1, \lambda_1\}\} \quad (2.1)$$

*in deterministic  $2^{O(n)}$  poly( $\cdot$ ) time and  $2^n$  poly( $\cdot$ ) space.*

### 3 CVP via Lattice Sparsification

To start, we give a precise definition of the lattice sparsifier.

**Definition 3.1** (Lattice Sparsifier). *Let  $K \subseteq \mathbb{R}^n$  be a  $\gamma$ -symmetric convex body,  $\mathcal{L}$  be an  $n$ -dimensional lattice and  $t \geq 0$ . A  $(K, t)$  sparsifier for  $\mathcal{L}$  is a sublattice  $\mathcal{L}' \subseteq \mathcal{L}$  satisfying*

1.  $\forall \mathbf{x} \in \mathbb{R}^n, d_K(\mathcal{L}', \mathbf{x}) \leq d_K(\mathcal{L}, \mathbf{x}) + t$
2.  $G(tK, \mathcal{L}) = 2^{O(n)} \gamma^{-n}$

The following theorem represents the formalization of our lattice sparsifier construction.

**Theorem 3.2** (Algorithm Lattice-Sparsifier). *Let  $K \subseteq \mathbb{R}^n$  be a  $(\mathbf{0}, r, R)$ -centered and  $\gamma$ -symmetric convex body specified by a weak membership oracle  $O_K$ , and let  $\mathcal{L}$  denote an  $n$  dimensional lattice with a basis  $B \in \mathbb{Q}^{n \times n}$ . For  $t \geq 0$ , a  $(K, t)$  sparsifier can be constructed for  $\mathcal{L}$  using  $2^{O(n)}$  poly( $\cdot$ ) time and  $2^n$  poly( $\cdot$ ) space.*

The proof of the above theorem is the subject of Sections 4 and 5 (randomized and deterministic constructions, respectively). Using the above lattice sparsifier construction, we present the following simple algorithm for  $(1 + \varepsilon)$ -CVP.

**Theorem 3.3.** *Algorithm 1 (Approx-Closest-Vectors) is correct, and on inputs  $K, \mathcal{L}, \mathbf{x}, \varepsilon$  (as above),  $K$   $\gamma$ -symmetric, it runs in deterministic  $2^{O(n)} \gamma^{-n} (1 + \frac{1}{\varepsilon})^n$  poly( $\cdot$ ) time and  $2^n$  poly( $\cdot$ ) space.*

*Proof.*

**Correctness:** If  $\mathbf{x} \in \mathcal{L}$ , we are clearly done. Next since  $K$  is  $(0, r, R)$ -centered, we have that  $\frac{\|\mathbf{y}\|}{R} \leq \|\mathbf{y}\|_K \leq \frac{\|\mathbf{y}\|}{r}$  for all  $\mathbf{y} \in \mathbb{R}^n$ . Now take any  $\mathbf{z} \in \text{CVP}(K, \mathcal{L}, \mathbf{x})$  and  $\tilde{\mathbf{z}} \in \text{SVP}(B_2^n, \mathcal{L})$ . Here we note that  $d_x = \|\mathbf{z} - \mathbf{x}\|_K$ . As in the algorithm, let  $l = \frac{\|\tilde{\mathbf{z}} - \mathbf{x}\|}{R}$ . Now we see that

$$l = \frac{\|\tilde{\mathbf{z}} - \mathbf{x}\|}{R} \leq \frac{\|\mathbf{z} - \mathbf{x}\|}{R} \leq \|\mathbf{z} - \mathbf{x}\|_K \leq \|\tilde{\mathbf{z}} - \mathbf{x}\|_K \leq \frac{\|\tilde{\mathbf{z}} - \mathbf{x}\|}{r} = l \frac{R}{r}$$

Therefore  $l \leq d_x \leq l \frac{R}{r}$ .

Let  $d_f$  denote the value of  $d$  after the first while loop terminates. We claim that  $\frac{1}{2}d_f \leq d_x \leq (1 + \varepsilon/3)d_f + \varepsilon_0$ . When the while loop terminates, we are guaranteed that the call to Lattice-Enum( $(1 + \frac{\varepsilon}{3})d_f K +$

---

**Algorithm 1** Approx-Closest-Vectors( $K, \mathcal{L}, \mathbf{x}, \varepsilon$ )

---

**Input:**  $(\mathbf{0}, r, R)$ -centered convex body  $K \subseteq \mathbb{R}^n$  with weak distance oracle  $D_K$  for  $\|\cdot\|_K$ , a basis  $B \in \mathbb{Q}^{n \times n}$  for  $\mathcal{L}$ , target  $\mathbf{x} \in \mathbb{Q}^n$ ,  $0 < \varepsilon \leq 1$

**Output:** Outputs a non-empty set  $S \subseteq \{\mathbf{y} \in \mathcal{L} : \|\mathbf{y} - \mathbf{x}\|_K \leq (1 + \varepsilon)d_K(\mathcal{L}, \mathbf{x})\}$

```
1: if  $\mathbf{x} \in \mathcal{L}$  then return  $\{\mathbf{x}\}$ 
2: Compute  $\mathbf{z} \in \text{CVP}(B_2^n, \mathcal{L}, \mathbf{x})$  using the MV algorithm
3:  $l \leftarrow \frac{\|\mathbf{z} - \mathbf{x}\|_2}{R}$ ;  $\varepsilon_0 \leftarrow \frac{\varepsilon}{9} \min\{1, l\}$ 
4:  $d \leftarrow \frac{l}{2}$ ;  $\tilde{d}_x \leftarrow \infty$ 
5: repeat
6:    $d \leftarrow 2d$ 
7:    $\mathcal{L}' \leftarrow \text{Lattice-Sparsifier}(K, \mathcal{L}, \frac{\varepsilon}{3}d)$ 
8:   for all  $\mathbf{y} \in \text{Lattice-Enum}((1 + \frac{\varepsilon}{3})dK + \mathbf{x}, \mathcal{L}', r\varepsilon_0)$  do
9:      $\tilde{d}_x \leftarrow \min\{\tilde{d}_x, D_{K, \varepsilon_0}(\mathbf{y} - \mathbf{x}), (1 + \frac{\varepsilon}{3})d + \varepsilon_0\}$ 
10: until  $\tilde{d}_x < \infty$ 
11: return  $\text{Lattice-Enum}((\tilde{d}_x + \varepsilon_0)K + \mathbf{x}, \mathcal{L}', r\varepsilon_0)$ 
```

---

$\mathbf{x}, \mathcal{L}', r\varepsilon_0$ ), outputs a lattice vector in  $\mathcal{L}'$  at distance at most  $(1 + \frac{\varepsilon}{3})d_f + \varepsilon_0$  from  $\mathbf{x}$ . Since  $\mathcal{L}' \subseteq \mathcal{L}$ , we clearly have that  $d_x \leq (1 + \frac{\varepsilon}{3})d_f + \varepsilon_0$  as needed.

If the while loop terminates after the first iteration, then  $d_f = l \leq d_x$  and hence  $\frac{1}{2}d_f < d_x$  as needed. If the loop iterates more than once, then for the sake of contradiction, assume that  $\frac{1}{2}d_f > d_x$ . Then in the last iteration, the value of  $d$  is greater than  $d_x$ . Now we are guaranteed that  $\text{Lattice-Sparsifier}(K, \mathcal{L}, \frac{\varepsilon}{3}d)$  returns a lattice  $\mathcal{L}'$  satisfying

$$d_K(\mathcal{L}', \mathbf{x}) \leq d_K(\mathcal{L}, \mathbf{x}) + \frac{\varepsilon}{3}d \leq (1 + \frac{\varepsilon}{3})d$$

But then the call to  $\text{Lattice-Enum}((1 + \frac{\varepsilon}{3})dK + \mathbf{x}, \mathcal{L}', r\varepsilon_0)$  is guaranteed to return a lattice point, and hence the while loop terminates at this iteration, a clear contradiction. Hence  $\frac{1}{2}d_f \leq d_x$  as needed.

Let  $d'_x = d_K(\mathcal{L}', \mathbf{x})$ , for  $\mathcal{L}'$  at the end of the while loop. We now claim that  $\tilde{d}_x$  (as in the algorithm) satisfies  $d'_x - \varepsilon_0 \leq \tilde{d}_x \leq d'_x + \varepsilon_0$ . We first note that  $\tilde{d}_x = \min\{d_f + \varepsilon_0, D_{K, \varepsilon_0}(\mathbf{z} - \mathbf{x})\}$  from some  $\mathbf{z} \in \mathcal{L}'$ . By the guarantees on  $D_{K, \varepsilon_0}$ , we get that

$$\tilde{d}_x = \min\{d_f + \varepsilon_0, D_{K, \varepsilon_0}(\mathbf{z} - \mathbf{x})\} \geq \min\{d'_x, \|\mathbf{z} - \mathbf{x}\|_K - \varepsilon_0\} \geq d'_x - \varepsilon_0,$$

as needed. For the second inequality, we examine two cases. First assume that  $\text{Lattice-Enum}(d_f K + \mathbf{x}, \mathcal{L}', r\varepsilon_0)$  outputs  $\mathbf{z} \in \text{CVP}(K, \mathcal{L}', \mathbf{x})$ . Then  $\tilde{d}_x \leq D_{K, \varepsilon_0}(\mathbf{z} - \mathbf{x}) \leq d'_x + \varepsilon_0$  as needed. If  $\text{Lattice-Enum}$  does not output any element of  $\text{CVP}(K, \mathcal{L}, \mathbf{x})$ , we must have that  $d_f < d'_x$  and hence  $\tilde{d}_x \leq d_f + \varepsilon_0 < d'_x + \varepsilon_0$ , as needed. Finally by the construction of  $\mathcal{L}'$ , we also have that  $d'_x \leq d_x + \varepsilon/3d_f \leq (1 + 2\varepsilon/3)d_x$ .

Since  $d'_x \leq \tilde{d}_x + \varepsilon_0$ , we know that  $((\tilde{d}_x + \varepsilon_0)K + \mathbf{x}) \cap \mathcal{L} \neq \emptyset$ . Therefore we are guaranteed that the final call to  $\text{Lattice-Enum}((\tilde{d}_x + \varepsilon_0)K + \mathbf{x}, \mathcal{L}', r\varepsilon_0)$  outputs all the closest vectors of  $\mathcal{L}'$  to  $\mathbf{x}$ . Finally, any vector  $\mathbf{y}$  outputted during this call satisfies

$$\|\mathbf{y} - \mathbf{x}\|_K \leq \tilde{d}_x + 2\varepsilon_0 \leq d'_x + 3\varepsilon_0 \leq (1 + 2\varepsilon/3)d_x + (\varepsilon/3)l \leq (1 + \varepsilon)d_x$$

as needed.



**Running Time:** We first bound the running time of each call to Lattice-Enum. Within the while loop, the calls to Lattice-Enum( $((1+\varepsilon/3)dK + \mathbf{x}, \mathcal{L}', r\varepsilon_0)$ ) run in  $2^{O(n)}G((1+\varepsilon/3)dK, \mathcal{L}') \text{poly}(\cdot)$  time and  $2^n \text{poly}(\cdot)$  space. By Lemma 2.1, since  $(1 + \varepsilon/3) = t(\varepsilon/3)$  for  $t = (3/\varepsilon + 1)$ , we have that

$$G((1 + \varepsilon/3)dK, \mathcal{L}') \leq (4t + 2)^n G((\varepsilon/3)d, \mathcal{L}') = 6^n (1 + 2/\varepsilon)^n G((\varepsilon/3)d, \mathcal{L}') = 2^{O(n)} \gamma^{-n} (1 + 1/\varepsilon)^n$$

since by the guarantees on Lattice-Sparsifier, we have that  $G((\varepsilon/3)d, \mathcal{L}') = \gamma^{-n} 2^{O(n)}$ . Next the final call to Lattice-Enum( $((\tilde{d}_x + \varepsilon_0)K + \mathbf{x}, \mathcal{L}', r\varepsilon_0)$ ) runs  $2^{O(n)}G((\tilde{d}_x + \varepsilon_0)K, \mathcal{L}') \text{poly}(\cdot)$  time and  $2^n \text{poly}(\cdot)$  space. Now note that  $\varepsilon_0 \leq \frac{1}{9}\varepsilon d_x$ , and hence  $(1 + \varepsilon/3)d_f \geq d_x - \varepsilon_0 \geq (1 - \varepsilon/9)d_x$ . From here we get that

$$d_f \geq \frac{1 - \varepsilon/9}{1 + \varepsilon/3} d_x \geq \frac{1 - 1/9}{1 + 1/3} d_x = 2/3 d_x$$

Finally,  $\tilde{d}_x + \varepsilon_0 \leq (1 + \varepsilon/3)d_f + 2\varepsilon_0 \leq (1 + \varepsilon/3)d_f + 2/9\varepsilon d_x \leq (1 + 2\varepsilon/3)d_f$ . Therefore, since  $(1 + 2\varepsilon/3) = t(\varepsilon/3)$  for  $t = (2 + 3/\varepsilon)$ , we get that

$$\begin{aligned} G((\tilde{d}_x + \varepsilon_0)d_f K, \mathcal{L}') &\leq G((1 + 2\varepsilon/3)d_f K, \mathcal{L}') \leq (4t + 2)^n G((\varepsilon/3)d_f, \mathcal{L}') \\ &= (10 + 12/\varepsilon)^n G((\varepsilon/3)d_f, \mathcal{L}') = 2^{O(n)} \gamma^{-n} (1 + 1/\varepsilon)^n \end{aligned}$$

by the guarantee on  $\mathcal{L}'$ .

Lastly, note that each call to Lattice-Sparsifier takes at most  $2^{O(n)} \text{poly}(\cdot)$  time and  $2^n \text{poly}(\cdot)$  space. Since the while loop iterates polynomially many times (i.e. at most  $\log_2(2R/r)$ ), the total runtime is  $2^{O(n)} \gamma^{-n} (1 + 1/\varepsilon)^n \text{poly}(\cdot)$  and the total space usage is  $2^n \text{poly}(\cdot)$  as needed.  $\square$

## 4 A Simple Randomized Lattice Sparsifier Construction

We begin with an existence proof for lattice sparsifiers using the probabilistic method. We will use the Cauchy-Davenport sumset inequality and another lemma in number theory about primegaps, a consequence of a theorem of Rosser and Schoenfeld [RS62, Nar00].<sup>4</sup>

**Theorem 4.1.** *Let  $p \geq 1$  be a prime. Then for  $A_1, \dots, A_k \subseteq \mathbb{Z}_p$ , we have that*

$$|A_1 + \dots + A_k| \geq \min\{p, \sum_{i=1}^k |A_i| - k + 1\}$$

**Lemma 4.2.** *For  $x > 1000$  there exists a prime  $p \in \mathbb{Z}$  satisfying  $x < p < \frac{4x}{3}$ .*

*Proof of Lemma 4.2 (Prime Gap).* We will use the bounds  $\pi(x) > x/\ln(x)$  if  $x > 17$ , and  $\pi(x) < 1.25506x/\ln(x)$  if  $x > 1$  where  $\pi(x)$  denotes the number of primes  $< x$  [RS62, Nar00]. If  $x > 1000$  then  $\pi(4x/3) > (4x/3)/\ln(4x/3) > 1.25506x/\ln(x) > \pi(x)$ , the lemma follows.  $\square$

We begin with the following crucial lemma. This forms the core of our lattice sparsifier construction.

**Lemma 4.3.** *Let  $p$  be a prime and  $S \subseteq \mathbb{Z}_p^n$  satisfying  $1000 < |S| < p < \frac{4|S|}{3}$  and  $\mathbf{0} \in S$ . Then there exists  $\mathbf{a} \in \mathbb{Z}_p^n$  satisfying*

1.  $|\{\mathbf{y} \in S : \langle \mathbf{y}, \mathbf{a} \rangle \equiv 0 \pmod{p}\}| \leq 6$
2.  $|\{\langle \mathbf{y}, \mathbf{a} \rangle \pmod{p} : \mathbf{y} \in S\}| \geq \frac{p+2}{3}$

*Proof.* Let  $\mathbf{a}$  denote a uniform random vector in  $\mathbb{Z}_p^n$ . We will show that  $\mathbf{a}$  satisfies both conditions (1) and (2) with non-zero probability. Let  $E_i^{\mathbf{y}}$  denote the indicator of the event  $\langle \mathbf{a}, \mathbf{y} \rangle \equiv i$  for  $\mathbf{y} \in S$  and  $i \in \mathbb{Z}_p$ .

<sup>4</sup>The authors are indebted to János Pintz for finding these references.

**Claim 1:**  $\mathbb{E}[\sum_{\mathbf{y} \in S \setminus \{\mathbf{0}\}} E_0^{\mathbf{y}}] = \frac{|S|-1}{p}$

*Proof.* By linearity of expectation it suffices to prove  $\mathbb{E}[E_0^{\mathbf{y}}] = \Pr[\langle \mathbf{a}, \mathbf{y} \rangle] = \frac{1}{p}$  for  $\mathbf{y} \in S \setminus \{\mathbf{0}\}$ . Since  $\mathbf{y} \neq \mathbf{0}$ ,  $p$  is a prime, and  $\mathbf{a}$  is uniform in  $\mathbb{Z}_p^n$  we have that  $\langle \mathbf{a}, \mathbf{y} \rangle$  is uniform in  $\mathbb{Z}_p$ . Therefore  $\Pr[\langle \mathbf{a}, \mathbf{y} \rangle] = \frac{1}{p}$ .  $\square$

**Claim 2:**  $\mathbb{E}[\sum_{\mathbf{x}, \mathbf{y} \in S, \mathbf{x} \neq \mathbf{y}} E_0^{\mathbf{x}-\mathbf{y}}] = \frac{|S|^2 - |S|}{p}$

*Proof.* If  $\mathbf{x} \neq \mathbf{y}$  then  $\mathbb{E} E_0^{\mathbf{x}-\mathbf{y}} = \frac{1}{p}$ . The Claim follows by the linearity of expectation.  $\square$

Now we will choose the vector  $\mathbf{a} \in \mathbb{Z}_p^n$ . By Markov's inequality

$$\Pr[|\{\mathbf{y} \in S \setminus \{\mathbf{0}\} : \langle \mathbf{a}, \mathbf{y} \rangle \equiv 0\}| < 6] \geq 1 - \frac{|S|-1}{6p} > \frac{5}{6}, \text{ and}$$

$$\Pr[|\{(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in S, \mathbf{x} \neq \mathbf{y}, \langle \mathbf{a}, \mathbf{x} \rangle \equiv \langle \mathbf{a}, \mathbf{y} \rangle\}| \leq \frac{6|S|}{5}] \geq 1 - \frac{5|S|^2 - 5|S|}{6|S|p} > \frac{1}{6}.$$

Hence there exists an  $\mathbf{a}$  such that both events hold. The first condition of the lemma is easy to check:

$$|\{\mathbf{y} \in S : \langle \mathbf{y}, \mathbf{a} \rangle \equiv 0\}| = |\{\mathbf{y} \in S \setminus \{\mathbf{0}\} : \langle \mathbf{y}, \mathbf{a} \rangle \equiv 0\}| + 1 \leq 5 + 1 = 6.$$

Now we will prove the second condition using our assumption and the Cauchy-Schwartz inequality:

$$\begin{aligned} \frac{11|S|}{5} &\geq |\{(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in S, \mathbf{x} \neq \mathbf{y}, \langle \mathbf{a}, \mathbf{x} \rangle \equiv \langle \mathbf{a}, \mathbf{y} \rangle\}| + |S| = |\{(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in S, \langle \mathbf{a}, \mathbf{x} \rangle \equiv \langle \mathbf{a}, \mathbf{y} \rangle\}| \\ &= \sum_{z \in \mathbb{Z}_p} |\{\mathbf{y} \in S : \langle \mathbf{a}, \mathbf{y} \rangle \equiv z\}|^2 \geq |S|^2 / |\{\langle \mathbf{y}, \mathbf{a} \rangle \pmod{p} : \mathbf{y} \in S\}|. \text{ These yield} \\ |\{\langle \mathbf{y}, \mathbf{a} \rangle \pmod{p} : \mathbf{y} \in S\}| &> \frac{5|S|}{11} > \frac{15p}{44} > \frac{p+2}{3}. \end{aligned} \quad \square$$

We give now our first lattice sparsifier construction. While this theorem is stated for symmetric norms only, it can be easily extended to general norms (see Lemma 5.2).

**Theorem 4.4.** *Let  $K \subseteq \mathbb{R}^n$  be a symmetric convex body,  $\mathcal{L} \subseteq \mathbb{R}^n$  an  $n$ -dimensional lattice, and  $t \geq 0$  a non-negative number. Let  $N = |tK \cap \mathcal{L}|$ , and take a prime  $p$  satisfying  $N < p < \frac{4N}{3}$  if  $N > 1000$  and  $p = 3$  otherwise. Then there exists  $\mathbf{w} \in \mathcal{L}^*$  such that the sublattice  $\mathcal{L}(\mathbf{w}) = \{\mathbf{y} \in \mathcal{L} : \langle \mathbf{w}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}$  satisfies*

$$1. \forall \mathbf{x} \in \mathbb{R}^n, d_K(\mathcal{L}(\mathbf{w}), \mathbf{x}) \leq d_K(\mathcal{L}(\mathbf{w}), \mathbf{x}) + 3t$$

$$2. G(3tK, \mathcal{L}(\mathbf{w})) \leq 1000 \cdot 7^n$$

*Proof.* If  $N \leq 1000$ , let  $\mathbf{w} = \mathbf{0}$ , so  $\mathcal{L}(\mathbf{0}) = \mathcal{L}$ . Condition (2) is trivially satisfied, and for condition (1) Lemma 2.1 implies

$$G(3tK, \mathcal{L}) \leq (2 \cdot 3 + 1)^n |tK \cap \mathcal{L}| \leq 1000 \cdot 7^n.$$

Now we assume that  $N > 1000$ . By Lemma 4.2 there exists a prime  $p$  satisfying  $N < p < \frac{4N}{3}$ , as required by the theorem. Let  $B^* = (\mathbf{b}^1, \dots, \mathbf{b}^n)$  denote a basis for  $\mathcal{L}^*$ . Set  $S = \{B^{*T} \mathbf{y} \pmod{p\mathbb{Z}^n} : \mathbf{y} \in tK \cap \mathcal{L}\}$ .

**Claim:**  $|\mathcal{L} \cap tK| = |S|$ .

*Proof.* Clearly  $|S| \leq |\mathcal{L} \cap tK|$ . We will prove  $|S| \geq |\mathcal{L} \cap tK|$  by contradiction: assume not and take  $\mathbf{y}_1, \mathbf{y}_2 \in \mathcal{L} \cap tK$ , where  $\mathbf{y}_1 - \mathbf{y}_2 \in p\mathcal{L}$ . Set  $\mathbf{y} = \mathbf{y}_1 - \mathbf{y}_2$ , so  $\mathbf{y} \in 2tK$ . Note that  $(k/p)\mathbf{y} \in \mathcal{L}$  for  $k \in \mathbb{Z}$  and

$$\|(k/p)\mathbf{y}\|_K = |k/p| \|\mathbf{y}\|_K \leq 2t |k/p|$$

by the symmetry of  $K$ . Hence for  $|k| \leq \lfloor p/2 \rfloor$  we get  $\|(k/p)\mathbf{y}\|_K \leq \frac{1}{2}2t = t$ , i.e.  $(k/p)\mathbf{y} \in tK$ . But then there are at least  $2\lfloor p/2 \rfloor + 1 \geq p > N$  distinct lattice points in  $\mathcal{L} \cap tK$ , a contradiction.  $\square$

Since  $\mathbf{0} \in S$ , and  $|S| < p < \frac{4|S|}{3}$ , by Lemma 4.3 there exists  $\mathbf{a} \in \mathbb{Z}_p^n$  s.t.  $|\mathbf{y} \in S : \langle \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}| \leq 6$  and  $|\langle \mathbf{a}, \mathbf{y} \rangle \pmod{p} : \mathbf{y} \in S| \geq \frac{p+2}{3}$ . Let  $\bar{\mathbf{a}}$  denote the unique representative of  $\mathbf{a}$  in  $\{0, \dots, p-1\}^n$ , and let  $\mathbf{w} = B^* \bar{\mathbf{a}}$ .

Let  $S_{in} = \{\mathbf{y} \in S : \langle \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}$  and  $C = \{\langle \mathbf{a}, \mathbf{y} \rangle \pmod{p} : \mathbf{y} \in S\}$ . We know that  $|S_{in}| \leq 6$  and  $|C| \geq \frac{p+2}{3}$  by our guarantees on  $\mathbf{a}$ . We establish condition (2) first. We know that  $|tK \cap \mathcal{L}(\mathbf{w})| = |S_{in}| \leq 6$ . Lemma 2.1 implies

$$G(3tK, \mathcal{L}(\mathbf{w})) \leq 7^n \cdot |tK \cap \mathcal{L}(\mathbf{w})| \leq 7^n \cdot 6 \leq 1000 \cdot 7^n.$$

Now we establish condition (1), i.e. for any  $\mathbf{x} \in \mathbb{R}^n$ ,  $d_K(\mathcal{L}(\mathbf{w}), \mathbf{x}) \leq d_K(\mathcal{L}, \mathbf{x}) + 3t$ . Let  $\mathbf{y} \in \mathcal{L}$  be (one of) the closest vector(s) to  $\mathbf{x}$ , i.e.  $d_K(\mathcal{L}, \mathbf{x}) = \|\mathbf{y} - \mathbf{x}\|_K$ . Since  $C \subseteq \mathbb{Z}_p$ ,  $|C| \geq \frac{p+2}{3}$  Theorem 4.1 yields

$$|C + C + C| \geq \min\{p, 3(\frac{p+2}{3} + 1) - 3\} \geq p,$$

and hence  $C + C + C = \mathbb{Z}_p$ . Therefore, there exists  $\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3 \in tK \cap \mathcal{L}$  and  $\mathbf{z} \in \mathcal{L}(\mathbf{w})$  satisfying  $\mathbf{y} = \mathbf{z} + \mathbf{y}_1 + \mathbf{y}_2 + \mathbf{y}_3$ . Finally, by the triangle inequality and the symmetry of  $K$  we get that  $\|\mathbf{z} - \mathbf{x}\|_K \leq \|\mathbf{y} - \mathbf{x}\|_K + \|\mathbf{z} - \mathbf{y}\|_K \leq d_K(\mathcal{L}, \mathbf{x}) + \sum_{i=1}^3 \|\mathbf{y}_i\|_K \leq d_K(\mathcal{L}, \mathbf{x}) + 3t$ , as needed.  $\square$

## 5 Derandomizing the Lattice Sparsifier Construction

We begin with a high level outline of the deterministic sparsifier construction. To recap, in the previous section, we build a  $(K, t)$  sparsifier for  $\mathcal{L}$  as follows

1. Compute  $N \leftarrow |tK \cap \mathcal{L}|$ . If  $N \leq 1000$  then return  $\mathcal{L}' = \mathcal{L}$ . Else find a prime  $p$  satisfying  $N < p < \frac{4N}{3}$ .
2. Build basis  $B^* \in \mathbb{Q}^{n \times n}$  for  $\mathcal{L}^*$  and compute  $S \leftarrow \{B^{*T} \mathbf{y} \pmod{p} : \mathbf{y} \in tK \cap \mathcal{L}\}$ .
3. Find a vector  $\mathbf{a} \in \mathbb{Z}_p^n$  satisfying (in fact, for slightly worse parameters, a random  $\mathbf{a} \in \mathbb{Z}_p^n$  succeeds with constant probability)

$$(a) \quad |\{\mathbf{y} \in S : \langle \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}| \leq 6 \quad (b) \quad |\{\langle \mathbf{a}, \mathbf{y} \rangle : \mathbf{y} \in S\}| \geq \frac{p+2}{3}$$

4. Return sublattice  $\mathcal{L}' = \{\mathbf{y} \in \mathcal{L} : \langle \mathbf{y}, B^* \mathbf{a} \rangle \equiv 0 \pmod{p}\}$ .

To implement the above construction efficiently and deterministically, we must overcome several obstacles. First, the number of lattice points  $N$  in  $tK \cap \mathcal{L}$  could be very large (since we have no control on  $t$ ). Hence we can not hope to compute  $N$  or the set  $S$  efficiently via lattice point enumeration. Second, the construction of the vector  $\mathbf{a}$  is probabilistic (see Lemma 4.3): we must replace this with an explicit deterministic construction.

To overcome the first difficulty, we will build the  $(K, t)$  sparsifier iteratively. In particular, we will compute a sequence of sparsifiers  $\mathcal{L}'_1, \dots, \mathcal{L}'_k$ , satisfying that  $\mathcal{L}'_{i+1}$  is a  $(K, c^i \lambda)$  sparsifier for  $\mathcal{L}'_i$  for  $i \geq 0$ , where  $\mathcal{L}'_0 = \mathcal{L}$ ,  $\lambda = \lambda_1(K, \mathcal{L})$  and  $c > 1$  is a constant. We start the sparsification process at the minimum distance of  $\mathcal{L}$ . We only increase the sparsification distance by a constant factor at each step. Hence we will be able to guarantee that the number of lattice points we process at each step is  $2^{O(n)}$ . Furthermore, the geometric growth rate in the sparsification distance will allow us to conclude that  $\mathcal{L}'_i$  is in fact a  $(K, \frac{c^{i+1}}{c-1} \lambda)$  sparsifier for  $\mathcal{L}$ . Hence, iterating the process roughly  $k \approx \ln \frac{t}{\lambda_1}$  times will yield the final desired sparsifier.

For the second difficulty, i.e. the deterministic construction of  $\mathbf{a}$ , the main idea is to use a dimension reduction procedure which allows  $\mathbf{a}$  to be computed efficiently via exhaustive enumeration (i.e. trying all

possible  $\mathbf{a}$ 's). Let  $N$  and  $S$  be as in the description. Since  $N < p < \frac{4N}{3}$ , we note that an exhaustive search over  $\mathbb{Z}_p^n$  requires a search over  $p^n \leq (\frac{4N}{3})^n$  possibilities, and the validity check (i.e. conditions (a) and (b)) for any particular  $\mathbf{a}$  can be implemented in  $\text{poly}(N)$  time by simple counting. Since the existence of the desired  $\mathbf{a}$  depends only on  $|S|$  and  $p$  (and not on  $n$ ), if we can compute a linear projection  $\pi : \mathbb{Z}_p^n \rightarrow \mathbb{Z}_p^{n-1}$  such that  $\pi(S) = |S|$ , then we can reduce the problem to finding a good  $\mathbf{a} \in \mathbb{Z}_p^{n-1}$  for  $\pi(S)$ . Indeed, such a map  $\pi$  can be computed efficiently and deterministically as long as  $n \geq 3$ . To see this, we first identify full rank  $n - 1$  dimensional projections with their kernels, i.e. lines in  $\mathbb{Z}_p^n$ . From here, we note that distinct elements  $\mathbf{x}, \mathbf{y} \in S$  collide under the projection induced by a line  $l$  iff  $\mathbf{x} - \mathbf{y} \in l$ . Since the total number of lines spanned by differences of elements in  $S$  is at most  $\binom{|S|}{2} < \binom{p}{2}$ , as long as there are at least  $\binom{p}{2}$  lines in  $\mathbb{Z}_p^n$  (i.e. for  $n \geq 3$ ) we can compute the desired projection. Therefore, repeating the process  $n - 2$  times, we are left with finding a good  $\mathbf{a} \in \mathbb{Z}_p^2$ , which we can do by trying all  $p + 1 < \frac{4N}{3} + 1$  lines in  $\mathbb{Z}_p^2$ . As discussed in the previous paragraph, we will be able to guarantee that  $N = 2^{O(n)}$ , and hence the entire construction described above can be implemented in  $2^{O(n)}$  time and space as desired.

## 5.1 Algorithms

We begin with the deterministic algorithm implementing Lemma 4.3. We denote the set of lines in  $\mathbb{Z}_p^n$  by  $\text{Lines}(\mathbb{Z}_p^n)$ . For a vector  $\mathbf{q} \in \mathbb{Z}_p^n$  we denote its orthogonal complement by  $\mathbf{q}^\perp = \{\mathbf{y} \in \mathbb{Z}_p^n : \langle \mathbf{q}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}$ .

---

### Algorithm 2 Algorithm Good-Vector( $S, p$ )

---

**Input:**  $S \subseteq \mathbb{Z}_p^n$ ,  $\mathbf{0} \in S$ , integer  $n \geq 1$ ,  $p$  a prime satisfying  $1000 < |S| < p < \frac{4|S|}{3}$ .

**Output:**  $\mathbf{a} \in \mathbb{Z}_p^n$  satisfying conditions of Lemma 4.3 .

```

1: if  $n = 1$ , return 1
2:  $P \leftarrow I_n$  ( $n \times n$  identity)
3: for  $n_0$  in  $n$  to 3 do
4:   for all  $\mathbf{q} \in \text{Lines}(\mathbb{Z}_p^{n_0})$  do
5:     Compute basis  $B \in \mathbb{Z}_p^{n_0 \times n_0 - 1}$  satisfying  $\mathbf{q}^\perp = B\mathbb{Z}_p^{n_0 - 1}$ 
6:      $\forall$  distinct  $\mathbf{x}, \mathbf{y} \in PS$  check that  $B^T \mathbf{x} \not\equiv B^T \mathbf{y} \pmod{p\mathbb{Z}_p^{n_0 - 1}}$ .
       If no collisions, set  $P \leftarrow B^T P$  and exit loop; otherwise, continue.
7: for all  $\mathbf{q} \in \text{Lines}(\mathbb{Z}_p^2)$  do
8:   Pick  $\mathbf{a} \in \mathbf{q} \setminus \{\mathbf{0}\}$ 
9:   Compute  $\text{zeros} \leftarrow |\{\mathbf{y} \in PS : \langle \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}|$ 
10:  Compute  $\text{distinct} \leftarrow |\{\langle \mathbf{a}, \mathbf{y} \rangle \pmod{p} : \mathbf{y} \in PS\}|$ 
11:  if  $\text{zeros} \leq 6$  and  $\text{distinct} \geq \frac{p+2}{3}$  then
12:    return  $P^t \mathbf{a}$ 
```

---

For the desired application of the algorithm given below, the set  $S$  above will in fact be represented implicitly. Here the main access methodology we will require from  $S$  is a way to iterate over its elements. In the context of  $(1+\varepsilon)$ -CVP, the enumeration method over  $S$  will correspond to the Lattice-Enum algorithm. Here we state the guarantees of the algorithm abstractly in terms of the number of iterations required over  $S$ .

**Theorem 5.1.** *Algorithm 2 is correct, and performs  $\text{poly}(n, \log p)p^4$  arithmetic operations and  $O(np^3)$  iterations over the elements of  $S$ . Furthermore, the space usage (not counting the space needed to iterate over  $S$ ) is  $\text{poly}(n, \log p)$ .*

*Analysis of Good-Vector.*

**Correctness:** We must show that the outputted vector  $\mathbf{a}$  satisfies the guarantees of Lemma 4.3:

1.  $|\{\mathbf{y} \in S : \langle \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}| \leq 6$
2.  $|\{\langle \mathbf{a}, \mathbf{y} \rangle \pmod{p} : \mathbf{y} \in S\}| \geq \frac{p+2}{3}$

If  $n = 1$  then setting  $\mathbf{a} \in \mathbb{Z}_p$  to 1 (i.e. line 1) trivially satisfies (1) and (2). We assume  $n \geq 2$ . We prove the following invariant for the first loop (line 2): at the beginning of each iteration,  $P \in \mathbb{Z}_p^{n_0 \times n}$  and  $|PS| = |S|$ .

First let us assume that during the loop iteration, we find  $B \in \mathbb{Z}_p^{n_0 \times (n_0-1)}$  satisfying  $B^T \mathbf{x} \neq B^T \mathbf{y}$  for all distinct  $\mathbf{x}, \mathbf{y} \in PS$  (verified in line 5). This yields that the map  $\mathbf{x} \rightarrow B^T \mathbf{x}$  is injective when restricted to  $PS$ , and hence  $|B^T PS| = |S|$ . Next, since  $B \in \mathbb{Z}_p^{n_0 \times (n_0-1)}$  and  $P \in \mathbb{Z}_p^{n_0 \times n}$ , we have that  $P$  is set to  $B^T P \in \mathbb{Z}_p^{(n_0-1) \times n}$  for the next iteration, as needed.

Now we show that a valid projection matrix  $B^T$  is guaranteed to exist as long as  $n_0 \geq 3$ . First, we claim that there exists  $\mathbf{q} \in \text{Lines}(\mathbb{Z}_p^{n_0})$ , such that for all distinct  $\mathbf{x}, \mathbf{y} \in PS$ ,  $(\mathbf{q} + \mathbf{x}) \cap (\mathbf{q} + \mathbf{y}) = \emptyset$ , i.e. all the lines passing through  $PS$  in the direction  $\mathbf{q}$  are disjoint. A line  $\mathbf{q}$  fails to satisfy (a) if and only if  $\mathbf{q} = \mathbb{Z}_p(\mathbf{x} - \mathbf{y})$  for distinct  $\mathbf{x}, \mathbf{y} \in PS$ . The number of lines that can be generated in this way from  $PS$  is at most  $\binom{|PS|}{2} = \binom{|S|}{2} < \frac{p(p-1)}{2}$ . Since  $|\text{Lines}(\mathbb{Z}_p^{n_0})| = \frac{p^{n_0}-1}{p-1} > \frac{p(p-1)}{2}$  for  $n_0 \geq 3$  we may pick  $\mathbf{q} \in \text{Lines}(\mathbb{Z}_p^{n_0})$  that satisfies (a). Now let  $B \in \mathbb{Z}_p^{n_0 \times (n_0-1)}$  denote a basis satisfying  $\mathbf{q}^\perp = B\mathbb{Z}_p^{n_0-1}$ . We claim that  $|B^T PS| = |PS|$ . Assume not, then there exists distinct  $\mathbf{x}, \mathbf{y} \in PS$  such that

$$B^T \mathbf{x} \equiv B^T \mathbf{y} \Leftrightarrow B^T(\mathbf{x} - \mathbf{y}) \equiv \mathbf{0} \Leftrightarrow (\mathbf{x} - \mathbf{y}) \in (B\mathbb{Z}_p^{n_0-1})^\perp = \mathbf{q},$$

which contradicts our assumption on  $\mathbf{q}$ . Therefore, the algorithm is indeed guaranteed to find a valid projection, as needed.

After the first for loop, we have constructed  $P \in \mathbb{Z}_p^{2 \times n}$  satisfying  $|PS| = |S|$ , where  $|S| < p < \frac{4|S|}{3}$ . By Lemma 4.3, there exists  $\mathbf{a} \in \mathbb{Z}_p^2$  satisfying (1) and (2) for the set  $PS$ . Since (1) and (2) holds for any non-zero multiple of  $\mathbf{a}$ , i.e. any vector defining the same line as  $\mathbf{a}$ , we may restrict the search to elements of  $\text{Lines}(\mathbb{Z}_p^2)$ . Therefore, by trying all  $p+1$  elements of  $\text{Lines}(\mathbb{Z}_p^2)$  the algorithm is guaranteed to find a valid  $\mathbf{a}$  for the  $PS$ . Noting that  $\langle \mathbf{a}, P\mathbf{y} \rangle \equiv \langle P^T \mathbf{a}, \mathbf{y} \rangle$ , we get that  $P^T \mathbf{a}$  satisfies (1) and (2) for the set  $S$ , as needed.

**Runtime:** For  $n = 1$  the runtime is constant. We assume  $n \geq 2$ . Here the first for loop is executed  $n - 2$  times. For each loop iteration we run through  $\mathbf{q} \in \text{Lines}(\mathbb{Z}_p^{n_0})$  until we find one inducing a good projection matrix  $B$ . From the above analysis, we iterate through at most  $\binom{|S|}{2} < \frac{p(p-1)}{2}$  elements  $\mathbf{q} \in \text{Lines}(\mathbb{Z}_p^{n_0})$  before finding a good projection matrix. For each  $\mathbf{q}$ , we build a basis matrix  $B$  for  $\mathbf{q}^\perp$  which can be done using  $\text{poly}(n, \log p)$  arithmetic operations. Next, we check for collisions against each pair  $\mathbf{x}, \mathbf{y} \in PS$ , which can be done using  $O(|S|) = O(p)$  iterations over  $S$ . Therefore, at each loop iteration we enumerate over  $S$  at most  $p^3$  times while performing only polynomial time computations. Hence, the total number of operations (excluding the time needed to output the elements of  $S$ ) is at most  $\text{poly}(n, \log p)p^4$ .

For the last phase, we run through the elements in  $\text{Lines}(\mathbb{Z}_p^2)$ , where  $|\text{Lines}(\mathbb{Z}_p^2)| = p + 1$ . The validity check for  $\mathbf{a} \in \text{Lines}(\mathbb{Z}_p^2)$  requires computing both the quantities (1) and (2). To compute  $|\{\mathbf{y} \in S : \langle \mathbf{y}, \mathbf{a} \rangle \equiv 0 \pmod{p}\}|$  we iterate once over the set  $S$  and count how many zero dot products there are. To compute  $|\{\langle \mathbf{a}, \mathbf{y} \rangle : \mathbf{y} \in S\}|$ , we first iterate over all residues in  $\mathbb{Z}_p$ . Next, for each residue  $i \in \mathbb{Z}_p$ , if we find  $\mathbf{y} \in S$  satisfying  $\langle \mathbf{a}, \mathbf{y} \rangle \equiv i \pmod{p}$ , we increment our counter by one, and otherwise continue. Hence for any specific  $\mathbf{a} \in \mathbb{Z}_p^2$ , we

iterate over the set  $S$  exactly  $p + 1$  times, performing  $\text{poly}(n, \log p)p^2$  operations. Hence, over the whole loop we perform  $O(p^2)$  iterations over the set  $S$ , and perform  $\text{poly}(n, \log p)p^3$  operations.

Therefore, over the whole algorithm we iterate over the set  $S$  at most  $np^3$  times, and perform at most  $\text{poly}(n, \log p)p^4$  operations. Furthermore, not counting the space needed to iterate over the set  $S$ , the space used by the algorithm is  $\text{poly}(n, \log p)$ .  $\square$

Before moving into the derandomized sparsifier construction, we show a simple equivalence between building a sparsifier for symmetric and asymmetric norms.

**Lemma 5.2.** *Let  $K$  be a  $\gamma$ -symmetric convex body, and let  $\mathcal{L}$  be an  $n$ -dimensional lattice. Take  $\mathcal{L}' \subseteq \mathcal{L}$ , a full dimensional sublattice. Then for  $t \geq 0$ , we have that  $\mathcal{L}'$  is a  $(K \cap -K, t)$  sparsifier  $\Rightarrow \mathcal{L}'$  is a  $(K, t)$  sparsifier.*

*Proof.* Let  $\mathcal{L}' \subseteq \mathcal{L}$  be a  $(K \cap -K, t)$  sparsifier. Since  $K \cap -K$  is 1-symmetric, by definition we have that  $G(t(K \cap -K), \mathcal{L}') = 2^{O(n)}$ . By Lemma A.1 and  $\gamma$ -symmetry of  $K$ , we have that

$$N(tK, t(K \cap -K)) = N(K, K \cap -K) \leq \frac{\text{vol}_n(K + \frac{1}{2}(K \cap -K))}{\text{vol}_n(\frac{1}{2}(K \cap -K))} \leq \frac{\text{vol}_n(\frac{3}{2}K)}{\text{vol}_n(\frac{1}{2}(K \cap -K))} \leq 3^n \gamma^{-n}$$

Therefore

$$G(tK, \mathcal{L}') \leq G(t(K \cap -K), \mathcal{L}')N(tK, t(K \cap -K)) = 2^{O(n)}3^n \gamma^{-n} = 2^{O(n)}\gamma^{-n} \text{ as needed.}$$

Since  $K \cap -K \subseteq K$ , we note that  $\|\mathbf{a}\|_K \leq \|\mathbf{a}\|_{K \cap -K}$  for all  $\mathbf{a} \in \mathbb{R}^n$ . Now take  $\mathbf{x} \in \mathbb{R}^n$ , and take  $\mathbf{z} \in \text{CVP}(K, \mathcal{L}, \mathbf{x})$ . By the guarantee on  $\mathcal{L}'$ , there exists  $\mathbf{y} \in \mathcal{L}'$  such that

$$\|\mathbf{y} - \mathbf{z}\|_{K \cap -K} \leq d_{K \cap -K}(\mathcal{L}', \mathbf{z}) + t = t$$

since  $\mathbf{z} \in \mathcal{L}$ . Next, using the triangle inequality we have that

$$\|\mathbf{y} - \mathbf{x}\|_K \leq \|\mathbf{y} - \mathbf{z}\|_K + \|\mathbf{z} - \mathbf{x}\|_K \leq \|\mathbf{y} - \mathbf{z}\|_{K \cap -K} + d_K(\mathcal{L}, \mathbf{x}) \leq d_K(\mathcal{L}, \mathbf{x}) + t$$

as needed. Therefore,  $\mathcal{L}'$  is a  $(K, t)$  sparsifier for  $\mathcal{L}$  as claimed.  $\square$

From the above lemma, we see that it suffices to build lattice sparsifiers for symmetric convex bodies, i.e. to build a  $(K, t)$  sparsifier it suffices to build a  $(K \cap -K, t)$  sparsifier for  $\mathcal{L}$ .

We now show how to use the Good-Vector algorithm to get a completely deterministic Lattice Sparsifier construction. The correctness and runtime of the algorithm given below yields the proof of Theorem 3.2.

*Proof of Theorem 3.2 (Lattice Sparsifier Construction).*

**Correctness:** We show that the outputted lattice is a  $(K, t)$  sparsifier for  $\mathcal{L}$ . By Lemma 5.2 it suffices to show that the algorithm outputs a  $(K \cap -K, t)$  sparsifier, which justifies the switch in line 2 from  $K$  to  $K \cap -K$ . In what follows, we therefore assume that  $K$  is symmetric.

We first claim that  $\lambda \leq 2\lambda_1(K, \mathcal{L})$ . To see by the guarantee on  $\text{Shortest-Vector}(K, \mathcal{L}, \frac{1}{3})$ , we have that  $\|\mathbf{y}\|_K \leq \frac{4}{3}\lambda_1(K, \mathcal{L})$ . This implies

$$\lambda \leq \frac{3}{2}\|\mathbf{y}\|_K \leq \frac{3}{2} \cdot \frac{4}{3}\lambda_1(K, \mathcal{L}) = 2\lambda_1(K, \mathcal{L}),$$

as needed.

---

**Algorithm 3** Algorithm Lattice-Sparsifier( $K, \mathcal{L}, t$ )

---

**Input:**  $(\mathbf{0}, r, R)$ -centered convex body  $K \subseteq \mathbb{R}^n$  with distance oracle  $D_K$ , for  $\|\cdot\|_K$ , basis  $B \in \mathbb{Q}^{n \times n}$  for  $\mathcal{L}$ , and  $t \geq 0$ .

**Output:**  $(K, t)$  sparsifier for  $\mathcal{L}$

```
1:  $K \leftarrow K \cap -K$ 
2: Compute  $\mathbf{y} \in \text{Shortest-Vectors}(K, \mathcal{L}, \frac{1}{3})$ 
3:  $\lambda \leftarrow D_{K, \frac{1}{2}}(\mathbf{y}); \varepsilon \leftarrow 7^{-(n+5)}$ 
4:  $k \leftarrow \lfloor \ln(\frac{2}{3}\frac{t}{\lambda} + 1) / \ln 3 \rfloor$ 
5:  $\mathcal{L}_0 \leftarrow \mathcal{L}; B_0 \leftarrow B$ 
6: for  $i$  in  $0$  to  $k - 1$  do
7:    $S \leftarrow \text{Lattice-Enum}(3^i(1 - \varepsilon)\lambda K, \mathcal{L}_i, \varepsilon\lambda r)$ 
8:   Compute  $N \leftarrow |S|$ 
9:   if  $N > 1000$  then
10:    Compute  $B_i^* \leftarrow B_i^{-T}$ , a basis for  $\mathcal{L}_i^*$ 
11:    Compute prime  $p$  satisfying  $N < p < \frac{4N}{3}$ 
12:     $\mathbf{a} \leftarrow \text{Good-Vector}(B_i^{*T} S \pmod{p\mathbb{Z}^n}, p)$ 
13:    Compute  $\mathcal{L}_{i+1} \leftarrow \{\mathbf{y} \in \mathcal{L}_i : \langle B_i^* \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}$  and basis  $B_{i+1}$  for  $\mathcal{L}_{i+1}$ 
14:   else
15:     $\mathcal{L}_{i+1} \leftarrow \mathcal{L}_i; B_{i+1} \leftarrow B_i$ 
16: return  $\mathcal{L}_k$ 
```

---

**Claim 1:** for each  $i$ ,  $0 \leq i \leq k$ , we have that

1.  $\forall \mathbf{x} \in \mathbb{R}^n, d_K(\mathcal{L}_i, \mathbf{x}) \leq d_K(\mathcal{L}, \mathbf{x}) + \frac{3}{2}(3^i - 1)\lambda$ .
2.  $G(3^i \lambda, \mathcal{L}_i) \leq 7^{n+4}$ .

*Proof.* We establish the claim by induction on  $i$ . For  $i = 0$ , we have that  $\mathcal{L}_0 = \mathcal{L}$ . Therefore,  $\mathcal{L}_0$  trivially satisfies property (1). Next, since  $\lambda \leq 2\lambda_1(K, \mathcal{L})$ , by Lemma 2.1 we have that  $G(\lambda K, \mathcal{L}_0) \leq (2 \cdot 2 + 1)^n = 5^n < 7^{n+4}$ . Hence  $\mathcal{L}_0$  also satisfies (2).

We now prove the claim for  $i \geq 1$ . Let  $S$  denote the set outputted by  $\text{Lattice-Enum}(3^{i-1}(1 - \varepsilon)\lambda K, \mathcal{L}_{i-1}, \varepsilon\lambda r)$ . By the guarantees on  $\text{Lattice-Enum}$ , the set  $S$  satisfies  $3^{i-1}(1 - \varepsilon)\lambda K \cap \mathcal{L}_{i-1} \subseteq S \subseteq (3^{i-1}(1 - \varepsilon)\lambda K + \varepsilon\lambda r B_2^n) \cap \mathcal{L}_{i-1}$ . Since  $r B_2^n \subseteq K$  and  $i \geq 1$  we have  $3^{i-1}(1 - \varepsilon)\lambda K + \varepsilon\lambda r B_2^n \subseteq 3^{i-1}\lambda K$ . Therefore,

$$3^{i-1}(1 - \varepsilon)\lambda K \cap \mathcal{L}_{i-1} \subseteq S \subseteq 3^{i-1}\lambda K \cap \mathcal{L}_{i-1} \quad (5.1)$$

Set  $N = |S|$  (line 8). By (5.1) and the induction hypothesis we have

$$|3^{i-1}(1 - \varepsilon)\lambda K \cap \mathcal{L}_{i-1}| \leq N \leq |3^{i-1}\lambda K \cap \mathcal{L}_{i-1}| \leq G(3^{i-1}\lambda K, \mathcal{L}) \leq 7^{n+4}$$

Assume  $N \leq 1000$ . Then the algorithm sets  $\mathcal{L}_i = \mathcal{L}_{i-1}$  and  $B_i = B_{i-1}$ . The induction hypothesis implies for  $\mathbf{x} \in \mathbb{R}^n$  that

$$d_K(\mathcal{L}_i, \mathbf{x}) = d_K(\mathcal{L}_{i-1}, \mathbf{x}) \leq d_K(\mathcal{L}, \mathbf{x}) + \frac{3}{2}(3^{i-1} - 1)\lambda \leq d_K(\mathcal{L}, \mathbf{x}) + \frac{3}{2}(3^i - 1)\lambda,$$

and hence  $\mathcal{L}_i$  satisfies (1). Next, by (5.1) we have that  $|3^i(1-\varepsilon)\lambda K \cap \mathcal{L}_i| \leq N \leq 1000$ . Therefore, Lemma 2.1 yields

$$\begin{aligned} G(3^{i+1}\lambda K, \mathcal{L}_{i+1}) &\leq (2 \cdot 3(1/(1-\varepsilon)) + 1)^n |3^i(1-\varepsilon)\lambda K \cap \mathcal{L}_{i+1}| \\ &\leq 7^n(1+2\varepsilon)^n \cdot 1000 \leq 7^{n+4}, \end{aligned}$$

where the last two inequalities follow since  $\varepsilon \leq 7^{-(n+5)}$ . Therefore  $\mathcal{L}_i$  satisfies requirement (2) as needed.

Assume  $N > 1000$ . Here we first compute  $N < p < \frac{4N}{3}$ , and a dual basis  $B_{i-1}^*$  for  $\mathcal{L}_{i-1}^*$ .

**Claim 2:**  $|B_{i-1}^{*T} S \pmod{p\mathbb{Z}^n}| = N$

*Proof.* Since  $|S| = N$ , if the claim is false, there exists distinct  $\mathbf{x}, \mathbf{y} \in \mathcal{L}$  such that

$$B_{i-1}^{*T} \mathbf{x} \equiv B_{i-1}^{*T} \mathbf{y} \pmod{p\mathbb{Z}^n} \Leftrightarrow B_{i-1}^{*T}(\mathbf{x} - \mathbf{y}) \equiv \mathbf{0} \pmod{p\mathbb{Z}^n} \Leftrightarrow \mathbf{x} - \mathbf{y} \in p\mathcal{L}_{i-1}.$$

Since  $\mathbf{x}, \mathbf{y} \in 3^{i-1}\lambda K$  and  $K$  is symmetric, we have that  $\mathbf{x} - \mathbf{y} \in 2 \cdot 3^{i-1}K \cap p\mathcal{L}_{i-1}$ . Let  $\mathbf{z} = \mathbf{x} - \mathbf{y} \in p\mathcal{L}_{i-1}$ . We examine the vector  $s\frac{\mathbf{z}}{p}$  for  $s \in \mathbb{Z}$  satisfying  $|s| \leq \lfloor \frac{p}{2} \rfloor = \frac{p-1}{2}$  (since  $p$  is odd). Since  $\frac{\mathbf{z}}{p} \in \mathcal{L}_{i-1}$ , we have that  $s\frac{\mathbf{z}}{p} \in \mathcal{L}_{i-1}$  and

$$\begin{aligned} s\frac{\mathbf{z}}{p} &\in \left\lfloor \frac{s}{p} \right\rfloor \cdot 2 \cdot 3^{i-1}K \subseteq \left( \frac{p-1}{2p} \right) 2 \cdot 3^{i-1}K = \left( 1 - \frac{1}{p} \right) 3^{i-1}K \\ &\subseteq (1-\varepsilon)3^{i-1}K, \end{aligned}$$

where the last inequality follows since  $p < \frac{4N}{3} \leq \frac{4}{3} \cdot 7^{n+4}$  and  $\varepsilon = 7^{-(n+5)}$ . Then, since  $s$  can take  $2\lfloor \frac{p}{2} \rfloor + 1 = p$  different values, the set  $(1-\varepsilon)3^{i-1}K$  contains at least  $p$  lattice points in  $\mathcal{L}_{i-1}$ . However, by the construction of  $N$ , we have that

$$|(1-\varepsilon)3^{i-1}K \cap \mathcal{L}_{i-1}| \leq N < p, \text{ a clear contradiction. The claim thus holds. } \square$$

Next, the algorithm computes  $\mathbf{a} \leftarrow \text{Good-Vector}(B_i^{*T} S \pmod{p\mathbb{Z}^n}, p)$ , and sets  $\mathcal{L}_i = \{\mathbf{y} \in \mathcal{L} : \langle B^* \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}$ . From Claim 2, equation 5.1 and the guarantees on Good-Vector, we get

1.  $|3^{i-1}(1-\varepsilon)\lambda K \cap \mathcal{L}_i| = |\{\mathbf{y} \in 3^{i-1}(1-\varepsilon)\lambda K \cap \mathcal{L}_{i-1} : \langle B^* \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}| \leq 6$ .
2.  $|\{\langle B^* \mathbf{a}, \mathbf{y} \rangle \pmod{p} : \mathbf{y} \in 3^{i-1}\lambda K \cap \mathcal{L}_{i-1}\}| \geq \frac{p+2}{3}$ .

From here, using the identical analysis as in Theorem 4.4, from (a) above we get that  $\forall \mathbf{x} \in \mathbb{R}^n$ ,  $d_K(\mathcal{L}_i, \mathbf{x}) \leq d_K(\mathcal{L}_{i-1}, \mathbf{x}) + 3 \cdot 3^{i-1}\lambda$ . The induction hypothesis on  $\mathcal{L}_{i-1}$  implies

$$d_K(\mathcal{L}_{i-1}, \mathbf{x}) + 3^i\lambda \leq d_K(\mathcal{L}, \mathbf{x}) + \frac{3}{2}(3^{i-1} - 1)\lambda + 3^i\lambda = d_K(\mathcal{L}, \mathbf{x}) + \frac{3}{2}(3^i - 1)\lambda.$$

Therefore  $\mathcal{L}_i$  satisfies (1) as needed. Using (b) and Lemma 2.1 we have that

$$\begin{aligned} G(3^i\lambda K, \mathcal{L}_i) &\leq (2 \cdot 3 \cdot (1/(1-\varepsilon)) + 1)^n |3^{i-1}(1-\varepsilon)\lambda K \cap \mathcal{L}_i| \\ &\leq 7^n(1+2\varepsilon)^n \cdot 6 < 7^{n+4}. \end{aligned}$$

Therefore  $\mathcal{L}_i$  satisfies (2). The claim thus follows.  $\square$



Given Claim 1, we will show that  $\mathcal{L}_k$  is a  $(K, t)$  sparsifier for  $\mathcal{L}$ . By our choice of  $k$ , note that  $\frac{3}{2}(3^k - 1)\lambda \leq t \leq 3 \cdot \frac{3}{2}(3^{k+1} - 1)\lambda$ . By the claim, for  $\mathbf{x} \in \mathbb{R}^n$ ,  $d_K(\mathcal{L}_k, \mathbf{x}) \leq d_K(\mathcal{L}, \mathbf{x}) + \frac{3}{2}(3^k - 1)\lambda \leq d_K(\mathcal{L}, \mathbf{x}) + t$ . It therefore only remains to bound  $G(tK, \mathcal{L}_k)$ . By the previous bounds

$$\frac{t}{3^k \lambda} \leq \frac{3(3^{k+1} - 1)\lambda}{2 \cdot 3^k \lambda} < \frac{9}{2}$$

Therefore, the claim and Lemma 2.1 imply

$$G(tK, \mathcal{L}_k) \leq (2 \cdot \frac{9}{2} + 1)^n G(3^k \lambda K, \mathcal{L}_k) \leq 10^n \cdot 7^{n+4} = 2^{O(n)}$$

as needed. The algorithm returns a valid  $(K, t)$  sparsifier for  $\mathcal{L}$ .

**Runtime:** The algorithm first runs the Shortest-Vectors on  $K$  and  $\mathcal{L}$ , which takes  $2^{O(n)} \text{poly}(\cdot)$  time and  $2^n \text{poly}(\cdot)$  space. Next, the for loop on line 6 iterates  $k = \lfloor \ln(\frac{2}{3}\frac{t}{\lambda} + 1) / \ln 3 \rfloor = \text{poly}(\cdot)$  times.

Each for loop iteration, indexed by  $i$  satisfying  $0 \leq i \leq k - 1$ , consists of computations over the set  $S \leftarrow \text{Lattice-Enum}(3^i(1 - \varepsilon)\lambda K, \mathcal{L}_i, \varepsilon\lambda r)$ . For the intended implementation, we do not store the set  $S$  explicitly. Every time the algorithm needs to iterate over  $S$ , we implement this by performing a call to  $\text{Lattice-Enum}(3^i(1 - \varepsilon)\lambda K, \mathcal{L}_i, \varepsilon\lambda r)$ . Furthermore, the algorithm only interacts with  $S$  by iterating over its elements, and hence the implemented interface suffices. Now at the loop iteration indexed by  $i$ , we do as follows:

1. Compute  $N = |S|$ . This is implemented by iterating over the elements of  $S$  and counting, and so by the guarantees of Lattice-Enum requires at most  $2^{O(n)} G(3^i \lambda K, \mathcal{L}_i) \text{poly}(\cdot) = 2^{O(n)} \text{poly}(\cdot)$  time (by Claim 1) and  $2^n \text{poly}(\cdot)$  space.
2. If  $N \leq 1000$ , we keep the same lattice and skip to the next loop iteration. If  $N > 1000$ , continue.
3. Compute  $B_i^* = B_i^{-T}$ . This can be done in  $\text{poly}(\cdot)$  time and space.
4. Compute a prime  $p$  satisfying  $N < p < \frac{4N}{3}$ . Such a prime can be computed by trying all integers in the previous range and using trial division. This takes at most  $O(N^2 \text{poly}(\log N)) = 2^{O(n)}$  time and  $\text{poly}(n)$  space.
5. Call  $\text{Good-Vector}(B^{T*} S \pmod{p\mathbb{Z}^n}, p)$ . By the guarantees on Good-Vector, the algorithm performs  $\text{poly}(n, \log p) p^4 = 2^{O(n)}$  operations and iterates at most  $np^3 = 2^{O(n)}$  times over the set  $B^{T*} S \pmod{p\mathbb{Z}^n}$ . These iterations can be performed  $2^{O(n)} \text{poly}(\cdot)$  time and  $2^n \text{poly}(\cdot)$  space by the guarantees on Lattice-Enum.
6. Compute a basis  $B_{i+1}$  for the new lattice  $\mathcal{L}_{i+1} = \{\mathbf{y} \in \mathcal{L}_i : \langle B^{*T} \mathbf{a}, \mathbf{y} \rangle \equiv 0 \pmod{p}\}$ . This can be done in  $\text{poly}(\cdot)$  time.

From the above analysis, we see that the entire algorithm runs in  $2^{O(n)} \text{poly}(\cdot)$  time and  $2^n \text{poly}(\cdot)$  space as needed.  $\square$

## 6 Further Applications and Future Directions

**Integer Programming.** We explain how the techniques in this paper apply to Integer Programming (IP), i.e. the problem of deciding whether a polytope contains an integer point, and discuss some potential associated venues for improving the complexity of IP. For a brief history, the first breakthrough works on IP are by Lenstra [Len83] and Kannan [Kan87], where it was shown that any  $n$ -variable IP can be solved in  $2^{O(n)} n^{2.5n}$  time (with polynomial dependencies on the remaining parameters). Since then, progress on IP has been slow, though recent complexity improvements have been made: the dependence on  $n$  was reduced to  $n^{2n}$  [HK10],  $\tilde{O}(n)^{\frac{4}{3}n}$  [DPV11], and finally  $n^n$  [Dad12a].

Let  $K \subseteq \mathbb{R}^n$  denote a polytope. To find an integer point inside  $K$ , the general outline of the above algorithms is as follows. Pick a center point  $\mathbf{c} \in K$ , and attempt to “round”  $\mathbf{c}$  to a point in  $\mathbb{Z}^n$  inside  $K$ . If this fails, decompose the integer program on  $K$  into subproblems. Here, the decomposition is generally achieved by partitioning  $\mathbb{Z}^n$  along shifts of some rational linear subspace  $H$  (often a hyperplane) and recursing on the integral shifts of  $H$  intersecting  $K$ .

In [Dad12b], an algorithm is given to perform the above rounding step in a “near optimal” manner. More precisely, the center  $\mathbf{c}$  of  $K$  is chosen to be the center of gravity  $\mathbf{b}$  of  $K$  (which can be estimated via random sampling), and rounding  $\mathbf{b}$  to  $\mathbb{Z}^n$  is done via an approximate CVP computation with target  $\mathbf{b}$ , lattice  $\mathbb{Z}^n$ , and norm  $\|\cdot\|_{K-\mathbf{b}}$  (corresponding to scaling  $K$  about  $\mathbf{b}(K)$ ). Here the AKS randomized sieve is used to perform the approximate CVP computation, which is efficient due to the fact that  $K - \mathbf{b}$  is near-symmetric (see [MP00]). Let  $\mathbf{y} \in \mathbb{Z}^n$  be the returned  $(1 + \varepsilon)$ -CVP solution, and assume that  $\mathbf{y}$  is correctly computed (which occurs with high probability). We can now examine the following cases. If  $\mathbf{y} \in K$ , we have solved the IP. If  $\|\mathbf{y} - \mathbf{b}\|_{K-\mathbf{b}} > (1 + \varepsilon)$ , then by the guarantee on  $\mathbf{y}$ , for any  $\mathbf{z} \in \mathbb{Z}^n$  we have that  $\|\mathbf{z} - \mathbf{b}\|_{K-\mathbf{b}} > 1 \Leftrightarrow \mathbf{z} \notin K$ . Hence, we can immediately decide that  $K \cap \mathbb{Z}^n = \emptyset$ . Lastly, if  $1 < \|\mathbf{y} - \mathbf{b}\|_{K-\mathbf{b}} \leq (1 + \varepsilon)$ , we know that  $\frac{1}{1+\varepsilon}K + \frac{\varepsilon}{1+\varepsilon}\mathbf{b}$  is integer free while  $(1 + \varepsilon)K - \varepsilon\mathbf{b}$  contains  $\mathbf{y}$ . In this final case, we are in essentially a near-optimal situation for computing a “good” decomposition (using the so-called “flatness” theorems in the geometry of numbers). We note with previous methods (i.e. using only symmetric norm or  $\ell_2$  techniques), the ratio of scalings between the integer free and non integer free case was  $O(n)$  in the worst case as opposed to  $(1 + \varepsilon)^2$  (here  $\varepsilon$  can be any constant  $\leq 1$ ).

With the techniques in this paper, we note that the above rounding procedure can be made Las Vegas (i.e. no probability of error, randomized running time) by replacing the AKS Sieve with our new DPV based solver (randomness is still needed to estimate the center of gravity). This removes any probability of error in the above inferences, making the above rounding algorithm easier to apply in the IP setting. We note that the geometry induced by the above rounding procedure is currently poorly understood, and very little of it is being exploited by IP algorithms. One hope for improving the complexity of IP with the above methods, is that with a strong rounding procedure as above one maybe able to avoid the worst case bounds on the number of subproblems created at every recursion node. Currently, the main way to show that  $K$  admits a small decomposition into subproblems is to show that the covering radius of  $K$  (i.e. the minimum scaling such that every shift of  $K$  intersects  $\mathbb{Z}^n$ ) is large. Using the above techniques, we easily get that in the final case the covering radius is  $\geq \frac{1}{1+\varepsilon}$  (since  $\frac{1}{1+\varepsilon}K + \frac{\varepsilon}{1+\varepsilon}\mathbf{b}$  is integer free), however in reality the covering radius could be much larger (yielding smaller decompositions). Here, an interesting direction would be to try and show that on the aggregate (over all subproblems), the covering radii of the nodes must grow as we go down the recursion tree. This would allow us to show that as we descend the recursion tree, the branching factor shrinks quickly, allowing us to get better bounds on the size of the recursion tree (which yields the dominant complexity term for current IP algorithms).

**CVP under  $\ell_\infty$ .** While the ideas presented here do not seem to be practically implementable in general (at least currently), there are special cases where the overhead incurred by our approach maybe acceptable. One potential target is solving  $(1 + \varepsilon)$ -CVP under  $\ell_\infty$ . This is one of the most useful norms that is often approximated by  $\ell_2$  for lack of a better alternative.

As an example, in [BC07], they reduce the problem of computing machine efficient polynomial approximations (i.e. having small coefficient sizes) of 1 dimensional functions to CVP under  $\ell_\infty$ . The goal in this setting is to generate a high quality approximation that is suitable for hardware implementation or for use in a software library, and hence spending considerable computational resources to generate it is justified.

We now explain why the  $\ell_\infty$  norm version of our algorithms maybe suitable for practical implementation (or at least efficient “heuristic” implementation). Most importantly, for  $\ell_\infty$  the DPV lattice point enumerator is trivial to implement. In particular, to enumerate the lattice points in a cube, one simply enumerates the points in the outer containing ball and retains those in the cube. Second, if one is comfortable with randomization, the sparsifier can be constructed by adding a simple random modular form to the base lattice. For provable guarantees, the main issue is that the modulus must be carefully chosen (see Section 4), however it seems plausible that in practice an appropriate modulus may be guessed heuristically.

## References

- [ABSS93] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *J. Comput. Syst. Sci.*, 54(2):317–331, 1997. Preliminary version in FOCS 1993.
- [AJ08] V. Arvind and P. S. Joglekar. Some sieving algorithms for lattice problems. In *FSTTCS*, pages 25–36. 2008.
- [Ajt98] M. Ajtai. The shortest vector problem in  $L_2$  is NP-hard for randomized reductions (extended abstract). In *STOC*, pages 10–19. 1998.
- [AKS01] M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *STOC*, pages 601–610. 2001.
- [AKS02] M. Ajtai, R. Kumar, and D. Sivakumar. Sampling short lattice vectors and the closest lattice vector problem. In *IEEE Conference on Computational Complexity*, pages 53–57. 2002.
- [Bab85] L. Babai. On Lovász’ lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986. Preliminary version in STACS 1985.
- [BC07] N. Brisebarre and S. Chevillard. Efficient polynomial l8 approximations. In *In Proceedings of the 18th IEEE Symposium on Computer Arithmetic*, pages 169–176. Society Press, 2007.
- [BN07] J. Blömer and S. Naewe. Sampling methods for shortest vectors, closest vectors and successive minima. In *ICALP*, pages 65–77. 2007.
- [CN98] J.-Y. Cai and A. Nerurkar. Approximating the SVP to within a factor  $(1+1/\dim^\varepsilon)$  is NP-hard under randomized reductions. *J. Comput. Syst. Sci.*, 59(2):221–239, 1999. Preliminary version in CCC 1998.
- [Dad12a] D. Dadush. *Integer Programming, Lattice Algorithms, and Deterministic Volume Estimation*. Ph.D. thesis, Georgia Institute of Technology, 2012.

- [Dad12b] D. Dadush. A  $o(\frac{1}{\varepsilon^2})$ -time algorithm for approximate integer programming. In *LATIN 2012*. 2012.
- [Din00] I. Dinur. Approximating  $\text{SVP}_\infty$  to within almost-polynomial factors is NP-hard. *Theor. Comput. Sci.*, 285(1):55–71, 2002. Preliminary version in CIAC 2000.
- [DKRS98] I. Dinur, G. Kindler, R. Raz, and S. Safra. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica*, 23(2):205–243, 2003. Preliminary version in FOCS 1998.
- [DPV11] D. Dadush, C. Peikert, and S. Vempala. Enumerative lattice algorithms in any norm via m-ellipsoid coverings. In *FOCS*. 2011.
- [DV12] D. Dadush and S. Vempala. Near optimal volume deterministic algorithms and lattice algorithms via m-ellipsoids. Arxiv, Report 1201.5972, 2012. <http://arxiv.org>.
- [EHN11] F. Eisenbrand, N. Hähnle, and M. Niemeier. Covering cubes and the closest vector problem. In *Proceedings of the 27th annual ACM symposium on Computational geometry*, SoCG ’11, pages 417–423. 2011.
- [FT87] A. Frank and v. Tardos. An application of simultaneous diophantine approximation in combinatorial optimization. *Combinatorica*, 7:49–65, 1987.
- [GMSS99] O. Goldreich, D. Micciancio, S. Safra, and J.-P. Seifert. Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Inf. Process. Lett.*, 71(2):55–61, 1999.
- [Hel85] B. Helfrich. Algorithms to construct minkowski reduced and hermite reduced lattice bases. *Theoretical Computer Science*, 41:125–139, 1985.
- [HK10] R. Hildebrand and M. Köppe. A faster algorithm for quasi-convex integer polynomial optimization. Arxiv, Report 1006.4661, 2010. <http://arxiv.org>.
- [HPS11] G. Hanrot, X. Pujol, and D. Stehlé. Algorithms for the shortest and closest lattice vector problems. In *Proceedings of the Third international conference on Coding and Cryptology*, IWCC’11, pages 159–190. Springer-Verlag, Berlin, Heidelberg, 2011.
- [HR07] I. Haviv and O. Regev. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. In *STOC*, pages 469–477. 2007.
- [HS07] G. Hanrot and D. Stehlé. Improved analysis of kannan’s shortest lattice vector algorithm. In *In CRYPTO*, pages 170–186. 2007.
- [JS98] A. Joux and J. Stern. Lattice reduction: A toolbox for the cryptanalyst. *J. Cryptology*, 11(3):161–185, 1998.
- [Kan87] R. Kannan. Minkowski’s convex body theorem and integer programming. *Mathematics of operations research*, 12(3):415–440, August 1987. 1987.
- [Kan92] R. Kannan. Lattice translates of a polytope and the frobenius problem. *Combinatorica*, 12:161–177, 1992.
- [Kho03] S. Khot. Hardness of approximating the shortest vector problem in high  $l_p$  norms. *J. Comput. Syst. Sci.*, 72(2):206–219, 2006. Preliminary version in FOCS 2003.

- [Kho04] S. Khot. Hardness of approximating the shortest vector problem in lattices. *J. ACM*, 52(5):789–808, 2005. Preliminary version in FOCS 2004.
- [KR95] M. Kaib and H. Ritter. Block reduction for arbitrary norms. Manuscript, 1995.
- [Len83] H. W. Lenstra. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8(4):538–548, November 1983.
- [LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, December 1982.
- [LS92] L. Lovász and H. E. Scarf. The generalized basis reduction algorithm. *Math. Oper. Res.*, 17(3):751–764, 1992. ISSN 0364-765X.
- [MG02] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, 2002.
- [Mic98] D. Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. *SIAM J. Comput.*, 30(6):2008–2035, 2000. Preliminary version in FOCS 1998.
- [MP00] V. Milman and A. Pajor. Entropy and asymptotic geometry of non-symmetric convex bodies. *Advances in Mathematics*, 152(2):314 – 335, 2000.
- [MV10] D. Micciancio and P. Voulgaris. A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations. In *STOC*, pages 351–358. 2010.
- [Nar00] W. Narkiewicz. *The Development of Prime Number Theory, From Euclid to Hardy and Littlewood*. Springer, 2000.
- [NS01] P. Q. Nguyen and J. Stern. The two faces of lattices in cryptology. In *CaLC*, pages 146–180. 2001.
- [Od190] A. M. Odlyzko. The rise and fall of knapsack cryptosystems. In C. Pomerance, editor, *Cryptography and Computational Number Theory*, volume 42 of *Proceedings of Symposia in Applied Mathematics*, pages 75–88. 1990.
- [RR06] O. Regev and R. Rosen. Lattice problems and norm embeddings. In *STOC*, pages 447–456. 2006.
- [RS62] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.
- [Sch87] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.*, 53:201–224, 1987.
- [Sch91] C. Schnorr. Factoring integers and computing discrete logarithms via diophantine approximation. In D. Davies, editor, *In EUROCRYPT*, Lecture Notes in Computer Science, pages 281–293. 1991.
- [VB99] E. Viterbo and J. Boutros. A universal lattice code decoder for fading channels. *IEEE Transactions on Information Theory*, 45:1639–1642, 1999.

[vEB81] P. van Emde Boas. Another NP-complete problem and the complexity of computing short vectors in a lattice. Technical Report 81-04, University of Amsterdam, 1981.

## A Covering Bound

In this section, we prove the basic covering bound stated in Lemma 2.1.

For a set  $A \subseteq \mathbb{R}^n$ , let  $\text{int}(A)$  denote the interior of  $A$ . For convex bodies  $A, B \subseteq \mathbb{R}^n$ , we define the covering number  $N(A, B) = \inf\{|\Lambda| : \Lambda \subseteq \mathbb{R}^n, A \subseteq \Lambda + B\}$ , i.e. the minimum number of translates of  $B$  needed to cover  $A$ . We will require the following standard inequality on the covering number.

**Lemma A.1.** *Let  $A, B \subseteq \mathbb{R}^n$  be convex bodies, where  $B$  is symmetric. Then*

$$N(A, B) \leq \frac{\text{vol}_n(A + B/2)}{\text{vol}_n(B/2)}.$$

*Proof.* Let  $T \subseteq A$  be any maximal set of points such that for all distinct  $\mathbf{x}, \mathbf{y} \in T$ ,  $(\mathbf{x} + B/2) \cap (\mathbf{y} + B/2) = \emptyset$ . We claim that  $A \subseteq T + B$ . For any  $\mathbf{z} \in A$ , note by maximality of  $T$  that there exists  $\mathbf{x} \in T$  such that  $(\mathbf{z} + B/2) \cap (\mathbf{x} + B/2) \neq \emptyset$ . Therefore  $\mathbf{z} \in \mathbf{x} + B/2 - B/2 = \mathbf{x} + B$ , as needed.

Since  $T + B/2$  corresponds to  $|T|$  disjoint translates of  $B/2$ , we have that

$$|T| \text{vol}_n(B/2) = \text{vol}_n(T + B/2) \leq \text{vol}_n(A + B/2).$$

Rearranging the above inequality yields the lemma.  $\square$

*Proof of Lemma 2.1.* We prove the bound on  $G(dK, \mathcal{L})$  in terms of  $\lambda_1(K \cap -K, \mathcal{L})$ .

Let  $s = \frac{1}{2}\lambda_1(K \cap -K, \mathcal{L})$ . For  $\mathbf{x} \in \mathcal{L}$ , we examine

$$\mathbf{x} + \text{int}(s(K \cap -K)) = \{\mathbf{z} \in \mathbb{R}^n : \|\mathbf{z} - \mathbf{x}\|_{K \cap -K} < s\}.$$

Now for  $\mathbf{x}, \mathbf{y} \in \mathcal{L}$ ,  $\mathbf{x} \neq \mathbf{y}$ , we claim that

$$\mathbf{x} + \text{int}(s(K \cap -K)) \cap \mathbf{y} + \text{int}(s(K \cap -K)) = \emptyset \tag{A.1}$$

Assume not, then  $\exists \mathbf{z} \in \mathbb{R}^n$  such that  $\|\mathbf{z} - \mathbf{x}\|_{K \cap -K}, \|\mathbf{z} - \mathbf{y}\|_{K \cap -K} < s$ . Since  $K \cap -K$  is symmetric, we note that  $\|\mathbf{y} - \mathbf{z}\|_{K \cap -K} = \|\mathbf{z} - \mathbf{y}\|_{K \cap -K} < s$ . But then we have that

$$\begin{aligned} \|\mathbf{y} - \mathbf{x}\|_{K \cap -K} &= \|\mathbf{y} - \mathbf{z} + \mathbf{z} - \mathbf{x}\|_{K \cap -K} \leq \|\mathbf{y} - \mathbf{z}\|_{K \cap -K} + \|\mathbf{z} - \mathbf{x}\|_{K \cap -K} \\ &< s + s = 2s = \lambda_1(K \cap -K, \mathcal{L}), \end{aligned}$$

a clear contradiction since  $\mathbf{y} - \mathbf{x} \neq 0$ .

Take  $\mathbf{c} \in \mathbb{R}^n$ . To bound  $G(dK, \mathcal{L})$  we must bound  $|(\mathbf{c} + dK) \cap \mathcal{L}|$ . For  $\mathbf{x} \in \mathbf{c} + dK$ , we note that  $\mathbf{x} + s(K \cap -K) \subseteq \mathbf{c} + (d + s)K$ . Therefore,

$$\begin{aligned} \text{vol}_n((d + s)K) &= \text{vol}_n(\mathbf{c} + (d + s)K) \geq \text{vol}_n((\mathbf{c} + dK) \cap \mathcal{L}) + \text{vol}_n(s(K \cap -K)) \\ &= |(\mathbf{c} + dK) \cap \mathcal{L}| \text{vol}_n(s(K \cap -K)) \end{aligned}$$

where the last equality follows from (A.1). Therefore, we have that

$$|(\mathbf{c} + dK) \cap \mathcal{L}| \leq \frac{\text{vol}_n((d + s)K)}{\text{vol}_n(s(K \cap -K))} = \left(\frac{d + s}{\gamma s}\right)^n = \gamma^{-n} \left(1 + \frac{2d}{\lambda_1(K \cap -K, \mathcal{L})}\right)^n$$

as needed.

We prove the bound on  $G(dK, \mathcal{L})$  in terms of  $|(K \cap -K) \cap \mathcal{L}|$ . Examine  $dK + \mathbf{x}$ . Let  $\mathbf{y}_1, \dots, \mathbf{y}_N \in (tK + \mathbf{x}) \cap \mathcal{L}$ , denote a maximal collection of points such that the translates  $\mathbf{y}_i + \frac{1}{2}(K \cap -K)$ ,  $i \in [N]$ , are interior disjoint. We claim that  $(dK + \mathbf{x}) \cap \mathcal{L} \subseteq \cup_{i=1}^N \mathbf{y}_i + (K \cap -K)$ . Take  $\mathbf{z} \in (dK + \mathbf{x}) \cap \mathcal{L}$ . Then by construction of  $\mathbf{y}_1, \dots, \mathbf{y}_N$ , there exists  $i \in [N]$  such that

$$\mathbf{z} + \frac{1}{2}(K \cap -K) \cap \mathbf{y}_i + \frac{1}{2}(K \cap -K) \neq \emptyset \Rightarrow \mathbf{z} \in \mathbf{y}_i + (K \cap -K)$$

as needed. Therefore  $|(dK + \mathbf{x}) \cap \mathcal{L}| \leq \sum_{i=1}^N |(\mathbf{y}_i + (K \cap -K)) \cap \mathcal{L}| = N|(K \cap -K) \cap \mathcal{L}|$ . Since  $K$  is  $\gamma$ -symmetric, we get that

$$N = \frac{\text{vol}_n(\cup_{i=1}^N \mathbf{y}_i + \frac{1}{2}(K \cap -K))}{\text{vol}_n(\frac{1}{2}(K \cap -K))} \leq 2^n \gamma^{-n} \frac{\text{vol}_n(dK + \frac{1}{2}(K \cap -K))}{\text{vol}_n(K)} \leq \gamma^{-n} (2d+1)^n$$

as needed. Since the above bound holds for all  $\mathbf{x} \in \mathbb{R}^n$ , we get that  $G(tK, \mathcal{L}) \leq \gamma^{-n} (2d+1)^n \cdot |(K \cap -K) \cap \mathcal{L}|$  as needed. □